Australian Government
Australian Institute of Criminology

AIC reports
Research Report 16

Online fraud victimisation in Australia: Risks and protective factors

Catherine Emami, Russell G Smith
and Penny Jorna

CRIMINOLOGY
RESEARCH GRANT

ISSN 2206-7280 (Online)
ISBN 978 1 922009 31 9 (Online)

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to stakeholder peer review.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Acknowledgements

This study was conducted with the cooperation and support of the Australian Competition and Consumer Commission (ACCC). The considerable expertise and assistance of the ACCC's Scamwatch staff are gratefully acknowledged.

Market research consultancy firm i-Link Research Solutions collected data for the sample of non-victims both professionally and efficiently. It provided a panel of individuals drawn from across Australia who were asked to complete the survey, and funding for this was provided by a Criminology Research Grant. Anthony Morgan, Research Manager at the Australian Institute of Criminology, kindly assisted with matched data analyses. The time and willingness of those who completed the survey are also gratefully acknowledged.

The opinions expressed in this publication are those of the authors alone and do not necessarily reflect the views or policies of the Australian Government or its entities.

Executive summary

Background

Online fraud occurs when an individual responds via the internet 'to a dishonest invitation, request, notification or offer by providing personal information or money that leads to a financial or non-financial loss or impact of some kind' (Cross, Smith & Richards 2014: 1). Examples of online fraud include dating or romance fraud, deceptive sales of products and services, dishonest investment schemes, lottery or inheritance schemes, working from home schemes (often a form of money laundering) or lottery fraud involving false prize draws or sweepstakes (Button et al. 2014; Button, Lewis & Tapley 2009; Chang 2008; Cross, Smith & Richards 2014).

Online fraud is a costly phenomenon not just in terms of its financial impact on business and government, but also because of the detrimental impact that it has on many of its victims. The total value of losses attributed to online consumer fraud in reports to the Australian Competition and Consumer Commission's (ACCC's) Scamwatch website in 2017 was more than $90m (ACCC 2018). While this figure is considerable, it is likely that the real financial impact of online consumer fraud is much higher, given many victims do not report their victimisation, some people do not even realise they have been defrauded or are unable to quantify their losses (Button, Lewis & Tapley 2009; Cross & Blackshaw 2014). The non-financial impact suffered by individual victims is often difficult to quantify (ACCC 2018).

To gain a better understanding of online consumer fraud, the Australian Institute of Criminology (AIC) partnered with the ACCC to identify and quantify the factors that make individuals vulnerable to consumer fraud and lead to their victimisation. This study aimed to replicate and develop research undertaken by the AIC in 2010 (Ross and Smith 2011) by using a larger sample of victims and comparing their vulnerabilities with a matched sample of non-victims.

Methodology

Two independent samples were used in the study. A victim sample was composed of individuals who had made a report to the ACCC's Scamwatch website between 1 January 2013 and 31 July 2015. A total of 5,308 emails inviting individuals to complete the AIC's questionnaire were sent by the ACCC between May and August 2015. Clear information was provided to ensure that recipients would be confident of the legitimacy of the research.

The first round of 4,629 emails was sent on 15 May 2015. Second and third mail-outs were conducted on 2 and 31 July 2015 to 329 and 350 potential respondents respectively. Of the 5,308 emails that were sent, 566 questionnaires were completed—a completion rate of 10.7 percent.

The same questionnaire that was administered to the ACCC sample was also administered to a separate independent control group of 1,271 individuals who had subscribed to an online research panel provided by i-Link Research Solutions, a commercial market research company. The control group was matched to the ACCC sample by combining the variables of age, gender and state/territory of residence.

The sample

The survey was intended to obtain information about the characteristics of respondents throughout Australia. Accordingly, the 30 respondents who indicated that they did not reside in Australia were excluded from the analysis. One other individual was excluded from the ACCC sample because of incomplete responses, leaving a total of 535 useable responses.

In relation to the control group, 71 respondents indicated that they had made a report to the ACCC about goods or services that they had attempted to buy online from overseas since 1 January 2013. These individuals were excluded from data analysis to ensure that this sample was independent of the victim sample.

Overall, 1,735 respondents completed the survey—535 respondents who had made a report to the ACCC and 1,200 control group respondents, with 203 victims and 321 non-victims ultimately being identified.

From the final sample (n=524) further sub-samples were created: a victim and non-victim sample (n=352, 176 from each category) matched (using exact matching) on age, gender and level of education attained; and a one-time victim and repeat victims sample (n=161, 58 repeat victims and 103 one-time victims).

Although the current victim sample was drawn from those who reported to the ACCC's Scamwatch portal, and the non-victim sample matched exactly with the victim sample on age, gender and level of education attained, some differences were observed between demographics of victims in the current sample and victims in the latest Scamwatch study (ACCC 2018). Higher proportions of Scamwatch victims were present in the lowest age group, among female victims, and from New South Wales, Queensland and the Northern Territory. These differences were also apparent between the current victims sample and the ACCC's data for 2014 (ACCC 2015).

Determining victimisation

The online questionnaire did not contain a specific question asking whether or not respondents had been the victims of an online fraud. Rather, respondents were asked if they had 'transferred money overseas' in the two years prior to participating in the survey; their purpose for sending money overseas; and if they were satisfied with the outcome of that undertaking (for example, were they satisfied with the goods or services they were expecting in return for the overseas payments). From these questions it was then determined whether or not it was likely that the respondent had been a victim of online fraud.

A group was created from a sub-set of the victim and non-victim sample, which consisted of 176 victims and 176 non-victims matched exactly on age, gender and educational attainment. Further analyses were conducted to examine any differences between the online behaviour of victims and non-victims.

Differences between victims and non-victims

The purpose for sending money overseas

Differences were identified concerning the purpose behind respondents deciding to send money overseas. The most frequent reason non-victims sent money overseas was to buy goods and services online. Victims were more likely to send money overseas for business transactions, or to friends they had met online compared with non-victims.

Victims were also more likely to send money to people they had not previously known than non-victims. In contrast to this, non-victims were more likely than victims to send money to relatives or friends other than those met online.

The reason respondents sent money overseas

Victims were more likely than non-victims (22% compared with 1%) to send money overseas based on a belief that they may gain a financial reward. Victims were also more likely than non-victims to have sent money overseas to help or assist someone they had met online (a common romance scam premise).

Non-victims were more likely to have sent money overseas to buy goods or services online; however, a small number of non-victims provided reasons that have also been commonly associated with online fraud, indicating they may have fallen victim to online fraud but had not realised that this was the case.

Amount sent overseas

Victims sent more money overseas during the last two years than non-victims, with 10.3 percent of victims sending between $10,001 and $20,000, and six percent sending between $20,001 and $40,000. By contrast, only three percent of non-victims sent between $5,001 and $10,000 and less than two percent of non-victims sent between $20,001 and $160,000.

Mann-Whitney U tests found the mean amount sent by victims was significantly more than the mean amount sent overseas by non-victims. This applied to both the total amount sent and the largest amount sent in the previous two years. This may be an important finding for scam disruption techniques and ways for banks and money transfer businesses to help identify victims.

Method of payment

Victims were found to be more likely to transfer funds electronically using methods of payment, such as electronic funds transfer or money wire transfer, than non-victims who did not use these methods. This association remained statistically significant after multivariate analysis. This finding reinforces the need for consumer protection campaigns and programs to educate and remind individuals of the risks associated with using money wire transfers when making overseas payments.

Researching the undertaking

Victims were more likely than non-victims to have conducted research prior to sending money overseas. However, when the types of research conducted by victims and non-victims were analysed there were substantial differences in the nature of the research undertaken. For example non-victims relied on online independent reviews of websites or products, whereas victims simply relied on the websites of the product or business in question.

Negative life events

Prior research (Ross and Smith 2011) has suggested people who have suffered some negative life events may be more likely to be victims of online fraud. Respondents were asked about whether they had experienced certain life events. The only negative life event which had a statistically significant association with online victimisation was a relationship or marriage breakdown. Victims were found to be more likely than non-victims to have experienced a relationship breakdown in the previous five years. However, further analysis revealed that this was not statistically significant in predicting online fraud victimisation.

Computer literacy and usage

Respondents were asked about their knowledge of, and ability to use computers and other types of information technology (IT). They were also asked about the types of internet security they used. No statistically significant relationships were found to exist between online victimisation and how respondents rated their knowledge of computers.

A relationship was found to exist between the ability to use computers and IT, and online fraud victimisation. A higher percentage of non-victims rated their ability as either 'high' or 'very high' compared with victims. Victims were statistically more likely to rate their ability to use computers and IT as very low, compared with non-victims.

A higher proportion of non-victims spent 10 hours or more using the internet each week than victims. Non-victims also used more advanced forms of online security, such as anti-phishing software and content and imaging filtering when online compared with victims.

Consequences of victimisation

Most victims (61%) indicated that they had lost confidence in other people as a result of their decision to send money overseas. Similarly, almost 60 percent of victims indicated that they had experienced financial hardship and/or emotional trauma as a result of their involvement in such an undertaking. Almost one quarter of victims indicated they feared using the internet following their victimisation.

A sub-section of the victim sample was identified as 'repeat victims' indicating they had sent money overseas multiple times and were dissatisfied with the outcome. As there is little research about the differences between one-off victims and repeat victims of online fraud, further analyses were undertaken to examine if there were differences in why they were sending money and what impacts they might experience.

- For the total amount sent overseas in the previous two years, repeat victims sent significantly more money overseas than one-off victims.
- Repeat victims were more likely than one-off victims to have experienced financial hardship as a result of online fraud victimisation.
- Similar to the differences between victims and non-victims, repeat victims were more likely to send money to people they did not know than one-off victims.
- One negative life event was found to have a significant association with repeat victimisation—a marriage or relationship breakdown in the past five years.

Policy implications

This study found several opportunities that policymakers and consumer affairs organisations may want to take advantage of to improve the targeting of online consumer fraud prevention and awareness-raising initiatives in the future:

- This study found that victims who thought they were researching opportunities prior to sending money overseas were actually undertaking ineffective research, as they were often restricting this research to websites that were linked with the goods or services in question rather than independent sites. One practical way to try to reduce online fraud victimisation could be to provide tips on how to conduct more thorough research about organisations and companies and how to use independent online review websites.
- This research also identified different ways in which victims and non-victims transferred money overseas, which could also be interpreted as early warning signs that people may be sending money to fraudsters. For example, victims used money transfer businesses and banks more than non-victims. These organisations could be asked to provide more detailed information to victims about online fraud and the risks associated with transferring money overseas.

Ultimately, the present research confirmed what is already known about online fraud victimisation—namely, that victims are more likely to transfer money to people they do not personally know, or have met online, whereas non-victims are more likely to transfer money overseas to family or friends, or to buy goods and services from known businesses. These findings further suggest that more could be done to enhance education and awareness in terms of identifying to whom people are sending money, and for what purpose. This type of education is, arguably, best undertaken in conjunction with banks and money transfer businesses that have the most direct involvement with potential victims of online fraud.

This study provides new data to support the development of targeted online fraud awareness-raising campaigns that would focus on the online behaviour most likely to lead to victimisation. Further research could be conducted to verify whether the factors that were found to be statistically significant predictors of victimisation in the present study remain so once account is taken of their presence before and after victimisation.

Introduction

Online consumer fraud takes place when an individual responds via the internet 'to a dishonest invitation, request, notification or offer by providing personal information or money that leads to a financial or non-financial loss or impact of some kind' (Cross, Smith & Richards 2014: 1). Online consumer fraud is a costly phenomenon not only in terms of its financial impact on business and government, but also because of the detrimental impact that it has on many of its victims. The total value of losses attributed to online consumer fraud in reports to the Australian Competition and Consumer Commission's (ACCC's) Scamwatch website in 2017 was more than $90m (ACCC 2018). While this figure is considerable, it is likely that the real financial impact of online consumer fraud is much higher, given many victims do not report their victimisation, some people do not even realise they have been defrauded or are unable to quantify their losses (Cross & Blackshaw 2014; Button, Lewis & Tapley 2009), and the non-financial impact suffered by individual victims is often difficult to quantify (ACCC 2018).

To gain a better understanding of online consumer fraud, the Australian Institute of Criminology (AIC) partnered with the ACCC to determine and quantify the factors that make individuals vulnerable to consumer fraud and lead to their victimisation. The study aimed to replicate and develop research undertaken in an AIC pilot study in 2010 (Ross and Smith 2011) using a larger sample of victims and comparing their vulnerabilities with the characteristics of a matched sample of non-victims.

The way that people use the internet for recreation or for buying goods and services raises a number of important questions relevant to their risk of being victimised, including why some people experience more problems than others as a result of their online interactions. The purpose of this study was to examine consumer experiences when using online services over a two-year period, and to use this information to identify the best ways to prevent online consumer fraud victimisation.

Role and functions of the ACCC

The ACCC is an independent Commonwealth statutory authority responsible for regulating marketplace competition and consumer affairs in Australia. It promotes fair-trading and competition among businesses and consumers, and provides valuable information to members of the Australian public about their rights under the *Competition and Consumer Act 2010* (Cth) (ACCC 2018).

In addition to its regulatory role, the ACCC plays an important part in educating businesses and the public about fraud that takes place in the community and steps that consumers can take to avoid falling victim to this type of conduct. The ACCC's Scamwatch website (https://www.scamwatch.gov.au) not only allows consumers to report suspected fraud, but also provides consumers with useful educational resources about different types of fraud that have been brought to the ACCC's attention. In addition, it provides consumers with advice about who to contact for further assistance if they have become a victim of consumer fraud, and provides the ACCC with a useful source of data for inclusion in its annual Targeting Scams report (ACCC 2018).

Prior research on online fraud and consumer victimisation

Fraud and dishonesty have always been present in society, even as far back as the 4th century. 'Bottomry fraud', for example, was said to have been invented by the ancient Greeks shortly after they created the concept of bottomry—a type of maritime insurance (Corby 2009).

Bottomry involved boat owners borrowing money from lenders prior to setting sail, with a view to paying back the lender when the boat safely arrived at its next port. The boat owner would use the profits obtained from selling wares at the port to make the repayments to the moneylender. If the boat sank before reaching the port, the lender would lose the money lent (Corby 2009). It was not long before insurance frauds were developed with some boat owners deciding to conceal their ships at foreign ports, or deliberately sinking their boats, and so keeping the money loaned to them (Corby 2009).

While insurance fraud continues to exist today, a diverse range of other frauds have been created in response to developments in business and technology. Online fraud is an example of one type of fraud that has been facilitated with the introduction of the internet and society's reliance on this technology. The widespread use of the internet as a means of conducting day-to-day activities has resulted in an almost unlimited global pool of potential fraud victims that criminals can now try to exploit for their own financial gain (Chang 2008; Pratt, Holtfreter & Reisig 2010; van Wilsem 2013).

Online fraud

Online fraud occurs when an individual uses the internet to provide funds or personal information in response to a deceptive online invitation, notification, offer or request, which subsequently causes the victim to incur a financial or other non-financial loss (Cross, Smith & Richards 2014). While the methods used by online fraudsters to defraud victims are diverse, the end goal is essentially the same—that is, to obtain something of value from the victims (be this personal information or money) through the use of deceptive and dishonest representations (Cross, Smith & Richards 2014). It has been suggested that the continuing fall in so-called 'traditional' crime may be accounted for by the displacement of crimes such as fraud from the offline to the online environment (Williams 2016).

Online fraud can take a number of different forms. Examples include dating or romance fraud, deceptive sales of products and services, dishonest investment schemes, inheritance schemes, working from home schemes (often a form of money laundering), or lottery fraud involving false prize draws or sweepstakes (Button et al. 2014; Button, Lewis & Tapley 2009; Chang 2008; Cross, Smith & Richards 2014). So-called syntactic methods that make use of technology such as malware, phishing, vishing or skimming often accompany fraudulent invitations and seek to mislead users into disclosing personal information, transferring funds, or having their personal information obtained electronically without their knowledge (Button et al. 2014; Chang 2008; Cross, Smith & Richards 2014). Many victims only become aware of their victimisation when they are notified by banks, credit agencies, debt collectors or police.

One of the most common methods used by those seeking to defraud victims online is advance fee fraud. In 2017, the two most common scam types reported to the ACCC involving victims losing money were upfront payment and advance fee frauds, and other buying and selling scams (ACCC 2018). Individuals may fall victim to advance fee fraud by responding to emails promising some type of substantial benefit or reward in return for a comparatively small upfront payment. Invariably, the promised benefit fails to arrive.

While some online frauds aim to extract money from their victims at the outset, others are conducted for the purpose of obtaining victims' personal information that can then be used to obtain money. Phishing is an example of this type of fraud, whereby fraudsters create convincing copies of legitimate websites or emails to mislead unsuspecting individuals into providing the requested personal information, either by email or by completing fabricated online payment forms. To ease any concerns the victim may have about the 'legitimacy' of the fraudulent email, the fraudsters may produce fraudulent documents or build imitation websites as alleged 'evidence' of the authenticity of the correspondence (Chang 2008). Studies have found that one of the main reasons that people respond to fraudulent invitations is because they appear to be from authoritative and/or legitimate sources (Button et al. 2014; Dhamija, Tygar & Hearst 2006).

Prevalence of online fraud

A number of studies have been undertaken to ascertain the prevalence of online fraud in the Australian community. In 2017, the ACCC's annual Targeting Scams report found that over $90m was lost as a result of consumer scams reported to the ACCC, with a further $340m lost by consumers in scams reported to other government agencies and the Australian Cybercrime Online Reporting Network or ACORN (ACCC 2018). The top three most reported scam categories of 2017 were phishing, identity theft and false billing scams which are focused on gathering personal information in order to steal money from victims at a later time. Combined reports to ACORN and the ACCC showed that the resulting monetary losses from the theft of personal information exceeded $45m (ACCC 2018).

Between 2007 and 2014, the AIC also carried out an annual Online Consumer Fraud Survey to gain a greater understanding of consumer fraud victimisation in Australia. The self-selected online survey targeted Australian residents who had received fraudulent invitations in the last year. Results from the 2014 survey indicated that 98 percent (n=844) of the 865 survey participants received at least one invitation in the 12 months prior to the survey, and that 25 percent (n=220) had responded to an invitation in the previous 12 months by either requesting more information, providing personal information, suffering a financial loss, or providing personal information and suffering a financial loss. The median amount reported lost to fraudulent invitations was $900, with a total financial loss of $230,708 (Jorna 2016a).

The Australian Bureau of Statistics (ABS) has also released statistics on the prevalence and costs of personal fraud in Australia. For the ABS surveys, the term 'personal fraud' encompassed identity theft, credit card fraud, and scam fraud. In its most recent report on personal fraud in Australia (ABS 2016), the ABS found that 8.5 percent of the Australian population aged over 15 years (n=1.6m) had experienced identity theft, credit card fraud, or scam fraud in 2014–15, with 75 percent of the personal fraud victims (n=1.2m) incurring a financial loss. The average amount lost was $2,100, with a median loss of $400 (ABS 2016).

The victimisation rate and the total financial loss incurred by victims as a result of personal fraud increased between the ABS Personal Fraud Survey that was conducted in 2010–11 (ABS 2012) and that conducted in 2014–15, with a victimisation rate of 6.7 percent and a total financial loss amount of $1.4b recorded in 2010–11 (ABS 2012), compared with a victimisation rate of 8.5 percent and total financial loss of $3b in 2014–15 (ABS 2016).

Susceptibility to online fraud

Although many online frauds are tailored to appeal to specifically targeted individuals—a phenomenon known as 'spear phishing' (ACCC 2015; Cross 2015; United Kingdom Office of Fair Trading 2006), it is possible for anyone to be approached and to become a victim of online fraud. Some researchers have observed that socio-demographic factors are not a reliable predictor of fraud victimisation because the perpetrators of fraud target people from any background (Pratt, Holtfreter & Reisig 2010). Accordingly, demographics alone cannot be used as a reliable predictor of whether or not a person is likely to become a fraud victim (Ross and Smith 2011).

In their study of individuals who had transferred money to Nigeria between April 2007 and March 2008, Ross & Smith (2011) noted that across studies, age was the only demographic variable that has been consistently found to have some predictive value in terms of fraud victimisation, although the age group at highest risk differed between studies. Ross & Smith (2011) found in their study that respondents aged 65 years or older were more likely to be a victim of 'other' types of advance fee fraud invitations (such as lottery frauds) with victims between the ages of 45 and 54 years most likely to be victims of dating fraud. Victims aged between 18 and 24 years were most likely to be victims of online transaction fraud, while people aged between 35 and 44 years were least likely to be victims (Ross and Smith 2011).

Lee and Soberon-Ferrer (1997) also examined whether certain characteristics of victims increased their vulnerability to market fraud. They found that sociodemographic factors such as age, education and marital status influenced a person's vulnerability to consumer fraud, but that race and gender were not significant factors.

Jorna (2016b) found a significant relationship between age and how a fraudulent invitation was received, in her study of age and consumer fraud victimisation in Australia. She found that respondents under the age of 25 years were more likely to receive fraudulent invitations via the internet than those in older age groups, with respondents aged over 55 years being more likely to receive an invitation via a landline telephone than other media (Jorna 2016b). Jorna (2016b) also found some statistically significant relationships between age and fraud victimisation. Respondents aged 65 years and over were significantly more likely to send money in response to a fraudulent invitation than those in other age groups, and respondents aged 45–55 years experienced significantly greater levels of victimisation in relation to dating and romance frauds.

Ross & Smith (2011) also found a statistically significant relationship between the type of fraud victimisation that individuals experienced and income levels. Specifically, victims who earned less than $20,000 were more likely to have been victims of advance fee fraud or online transaction fraud, while individuals earning between $20,000 and $40,000 were more likely to have been victims of dating fraud. Individuals who earned more than $40,000 were less likely to be fraud victims than those in other income level categories.

It is difficult to pinpoint the precise personal factors that may contribute to a person's susceptibility to falling victim to online fraud. As noted by Cross (2015), victims of online fraud are often viewed in a negative way. Indeed, in some cases the victim is actually blamed for falling victim to the scam—their victimisation being attributed to ignorance or greed. However, Atkins and Huang (2013) have suggested that contrary to this belief, a person's vulnerability to online fraud is actually linked to the ability of fraudsters to skilfully manipulate human weaknesses to achieve their desired objectives. This use of manipulative and deceptive techniques to persuade people to perform particular actions has been described as 'social engineering' (Atkins & Huang 2013; Nhan, Kinkade & Burns 2009). This is a key methodology of consumer fraud.

Theoretical frameworks

Several theoretical perspectives can be applied to consumer fraud to help understand why people engage in and fall victim to this type of activity. These include Self-Control Theory (Gottfredson & Hirschi 1990), Routine Activity Theory (Cohen & Felson 1979), and Lifestyle-Exposure Theory (Hindelang, Gottfredson & Garofalo 1978).

Self-Control Theory

Self-Control Theory, devised by Gottfredson and Hirschi (1990), suggests that individuals with low self-control are more likely to commit crime than those who have higher levels of self-control due to their higher regard for their own self-interest rather than any long-term consequences of their actions (Gottfredson & Hirschi 1990; Ross & Smith 2011). Crime often provides perpetrators with instant gratification, thus fulfilling the offender's own self-interest in a relatively easy or simple way (Gottfredson & Hirschi 1990).

This would appear to make sense in the context of online fraud offending, insofar as offenders are seeking to obtain a benefit such as personal information (which may be used in the commission of more serious criminal activity at a later stage) or money from their victims, with little regard for the welfare of the victim or the long-term consequences of their actions.

The same reasoning can also be applied to victims of fraud (Holtfreter, Reisig & Pratt 2008) insofar as individuals with low self-control have been found to be more likely to:

> "…make impulsive decisions and engage in risky behaviours that are associated with negative life outcomes. As a result, they are more likely to act on opportunities that promise an immediate return with little effort or investment (Holtfreter et al. 2010: 200).

Holtfreter et al. (2010) suggested that it is this need for instant gratification that may explain why some individuals appear to be more susceptible to fraud victimisation than others. These findings are also consistent with research by Van Wyk and Benson (1997) who found that individuals who were willing to take financial risks were also more likely to report that they had been victims of fraud.

Self-Control Theory provides a useful framework for understanding online fraud in the context of the present research. For example, one of the characteristics of fraud victims that the present study sought to examine was whether there was a relationship between individuals who indicated they may have lower levels of self-control and the risk of online fraud victimisation—for instance, those victims who indicated that they were likely or very likely to make impulsive decisions, or that the main reason they decided to send money overseas was because they wanted to make extra money or gain a financial reward.

Routine Activity Theory

Cohen and Felson's (1979) Routine Activity Theory (RAT) provides another useful framework for understanding why it is that some people fall victim to online fraud and others do not. This theory suggests that crime takes place when motivated offenders and suitable targets cross paths in the absence of capable guardians who could intervene to prevent the crime occurring (Cohen & Felson 1979). The theory is often used to explain property and street crimes; however, it has also been found to apply to crimes such as online fraud and other crime types that take place in a cyber or virtual environment (Yar 2005).

If RAT is applied to online fraud offending, this fraud will take place when a motivated offender (the fraudster) comes into contact with a suitable target (the online victim) in the absence of capable guardians such as regulators or police (Cohen & Felson 1979). The interconnected nature of the world due to the internet means that there are now millions of potential victims for fraudsters to target anywhere around the world (Hutchings & Hayes 2009). Individuals who spend long periods of time on the internet each week may be at particular risk of falling victim to online fraud, given that the more time they spend undertaking this activity as part of their routine, the more likely they are to be exposed to motivated offenders (Ross and Smith 2011).

The role of a capable guardian in the context of RAT is to act as a deterrent to victimisation. Without capable guardianship there is no-one or nothing to stop the victimisation from taking place. While a capable guardian could take the form of adequate computer and internet security measures, it is also possible for a capable guardian in this context to take several other forms. Hutchings and Hayes (2009: 4) note:

> "The term 'capable guardian' is used widely; it may include the owner of the property (in the context of phishing, the account holder), law enforcement, Computer Emergency Response Teams (CERTs), banks and financial institutions, or any other individual or agency that has the potential to discourage offenders.

The RAT provides a useful framework for understanding online fraud in this study, which looks at whether a relationship could be found between the risk of online fraud victimisation and the routine activities of victims. In line with this theory, respondents were asked questions about the amount of time they spent on the internet each week and the computer security measures they used.

Lifestyle-Exposure Theory

Lifestyle-Exposure Theory (Hindelang, Gottfredson & Garofalo 1978) is similar to the RAT, and suggests that differences in individuals' lifestyles (the activities an individual undertakes for leisure and as part of their routine daily activities) in conjunction with certain demographic characteristics help to determine whether a person will become a victim of crime (Bernard, Snipes & Gerould 2010; Hindelang, Gottfredson & Garofalo 1978). Specifically, Hindelang, Gottfredson and Garofalo (1978) found that victimisation was closely linked to certain demographic characteristics of victims such as age, gender, marital status, income and race. These demographics are important in determining an individual's social roles and position within society and their subsequent lifestyle/s.

Young, single males from lower socioeconomic backgrounds were found to be at greater risk of victimisation than individuals with different demographic characteristics. Hindelang, Gottfredson and Garofalo (1978) suggested that this was because individuals in these higher-risk demographic groups were more likely to have lifestyles that would increase the possibility of these individuals associating or coming into contact with offenders.

Lifestyle-Exposure Theory may provide a useful framework for understanding online fraud in the context of the present research—specifically, whether there were any differences in the lifestyles and demographics of victims and non-victims (such as the amount of time they spent on the internet each week) that may have contributed to the risk of online fraud victimisation.

Negative life events

Certain negative life events may affect the likelihood of individuals becoming victims of crime. Consumer fraud victimisation is particularly pertinent due to the impact that negative life events can have on an individual's cognitive judgment and their ability to subsequently process information and make sound decisions (Lee & Soberon-Ferrer 1997). Negative life events, such as those involving a loss of some kind, can place considerable psychological stress on individuals. Such stress may adversely affect their risk-taking behaviour and impede their ability to face consumer roles if they are forced to make a decision during such a period of vulnerability (Chang & Chong 2010; Lee & Soberon-Ferrer 1997; Ross & Smith 2011).

It has been suggested that perpetrators of fraud actually make the most of the impact that negative life events can have on people's lives by relying on '…cognitive biases or errors in the mental process to initiate and execute their attacks and produce automatic emotional responses in their victims…' (Atkins & Huang 2013: 24). Cross (2015) has made a similar observation, noting that fraudsters frequently rely on identifying a victim's weaknesses, which they then exploit for the desired benefit or reward.

Shadel, Pak and Sauer (2014) found victims of fraud were more likely to report experiencing negative life events such as a negative change in financial status, divorce, or a serious illness or injury to themselves compared with non-victims (Shadel, Pak & Sauer 2014). Ross & Smith (2011) also suggest that unfortunate life events can have a negative impact on the ability of individuals to make sound judgments, which in turn, can increase their chances of falling victim to fraud, including online fraud.

Other studies have also found a link between fraud victimisation and recent experiences of negative life events. For instance, Anderson (2013) found that individuals who had experienced a serious negative life event such as a divorce, the death of a family member or close friend, a serious injury or illness in their family, or the loss of a job, were more than two-and-a-half times as likely to have experienced fraud compared with those who had not suffered these types of negative events. Those who had experienced a serious negative life event were also almost four times more likely to have fallen victim to debt-related fraud (ie advance fee loans, mortgage and credit relief schemes), and three times as likely to have been a victim of a fraudulent prize promotion compared with those individuals who had not experienced these negative life events (Anderson 2013).

Methodology

Purpose of the research

The purpose of this research was to determine and quantify the factors that make an individual vulnerable to online fraud and lead to his/her victimisation. Identifying these factors will help to inform the design of preventive measures and the development of targeted awareness-raising programs to minimise risks of online fraud victimisation in the future.

The dependent variable in this study was victimisation. Respondents were classified as victims if they indicated that they had sent money overseas in the last two years and were dissatisfied with the goods or services received in return for the payment that was made. Respondents were classified as non-victims if they had sent money overseas and were satisfied with the goods or services received in exchange for the money sent. This research focused on people who had sent money overseas as this is the principal way in which online consumer fraud victimisation occurs. The design of the study was also based on the research conducted by Ross & Smith (2011) that focused on individuals who had sent money overseas in response to advance fee fraud invitations.

The independent variables in this study were the characteristics of victims and certain life events that they may have experienced which could have increased their risk of becoming victims of online fraud. These included respondents' demographic details such as age, gender and place of residence, as well as whether they had experienced negative life events such as depression, a serious illness or injury, or the loss of employment. These demographic and other details were selected on the basis of prior research indicating their relevance for further testing.

Research design

A structured quantitative survey was used to track the process of fraud victimisation and to examine if there were any characteristics that could be identified as increasing an individual's risk of online fraud victimisation. This methodology replicated a similar study that was completed by Ross & Smith in 2011 that sought to identify risk factors for advance fee fraud victimisation (Ross and Smith 2011). Further information regarding the sampling used in this research project is outlined below.

Participants were invited to complete an online survey that contained a mixture of closed response and some open-ended questions. The survey was designed to be easy to administer and require little effort on the part of participants to access and complete.

The survey instrument was designed in conjunction with ACCC staff who had experience in dealing with victims of fraud through their role in receiving reports of fraudulent activity via the Scamwatch website.

The survey design was based on case-control studies so that two distinct samples could be observed—those who were victims of online fraud, and those who were not victims. From the remaining victim and non-victim samples a matched sample was created to emulate case-control studies used in epidemiology research. A case-control study is retrospective insofar as the outcome is known. In this case, the outcome was online fraud victimisation, and researchers work back to see which exposures might contribute to victimisation. The first step was to create a case group, consisting of victims of online fraud identified by the ACCC who had completed the online survey, and a control group from the panel group who were not victims. It was necessary for both groups to have sent money overseas in the previous two years prior to completing the survey. The participants may have sent money overseas for a variety of reasons, such as purchasing goods or providing money to friends or relatives. Victimisation was determined based on how satisfied participants were with the outcome of sending money. The research study was designed this way to compare similarities and differences between the groups so as to examine if there were any factors that may have contributed to the victimisation of respondents.

Questionnaire design

All respondents were asked a series of questions about their background and demographics, as well as their exposure to approaches made by persons unknown to them through electronic media seeking assistance in return for financial reward, and their responses to these approaches. Respondents were also asked questions regarding particular characteristics they may possess as well their experiences of certain negative life events.

Additional information was collected on known risk factors for consumer fraud in line with the theoretical frameworks of Lifestyle-Exposure Theory (Hindelang, Gottfredson & Garofalo 1978), Self-Control Theory (Gottfredson & Hirschi 1990) and Routine Activity Theory (Cohen & Felson 1979) discussed above.

Respondents were asked to provide demographic details such as their age, gender, education and income level. These details were obtained because according to Lifestyle-Exposure Theory (Hindelang, Gottfredson & Garofalo 1978), differences in individuals' lifestyles (the activities an individual undertakes for leisure and those they partake in as part of their routine daily activities) in conjunction with certain demographic characteristics, play a role in determining whether a person is likely to become a victim of crime (Hindelang, Gottfredson & Garofalo 1978).

Respondents were also asked several questions about negative life events they may have experienced to determine whether there was any relationship between the risk of online fraud victimisation and experiencing such events. Some of the negative life events that respondents were asked about included whether they had lost their job in the last five years, suffered from depression in the last five years, or been diagnosed with a serious illness in the last five years. These events were selected due to the fact that previous research has found a link between online fraud victimisation and experiencing such events (Anderson 2013; Ross & Smith 2011).

Respondents were also asked a number of questions about the amount of time they spent on the internet each week, and the computer security measures they used. The purpose of these questions was to examine whether a relationship could be found between one's risk of online fraud victimisation and their routine activities, or the guardianship tools they use (computer use being an example of the former, and computer security measures being an example of the latter). These questions were based on Cohen and Felson's (1979) Routine Activity Theory which suggests that crime takes place when motivated offenders and suitable targets cross paths in the absence of capable guardians who could intervene to prevent the crime occurring (Cohen & Felson 1979).

The questionnaire completed by the ACCC sample had 41 questions. The questionnaire given to the control group had 42 questions as it contained a screening question that asked respondents whether they had made a report to the ACCC about goods or services that they had attempted to buy online from overseas after 1 January 2013. The purpose of this question was to determine eligibility for inclusion in the sample, with individuals who indicated that they had made a report to the ACCC during this time period excluded so as to ensure that the sample remained independent.

Participation in the survey was completely voluntary and took 10–20 minutes to complete. Participants could end their participation in the survey at any stage, in which case their responses were not saved. No information that could later be used to identify respondents was sought from them. A copy of the questionnaire is attached at *Appendix A*.

Sampling framework

Two sampling frameworks were used to ensure good representation in both the victim and the non-victim cohorts and so that the differences between the two groups could be analysed.

Officers from the ACCC identified the victim sample based on individuals who had lost at least $300 and made a report to the ACCC's Scamwatch website after 1 January 2013. This date was chosen in the hope that victims would be better able to remember their victimisation and the subsequent impact it had on them if it took place within the last two years. It was also necessary to ensure that contact details for participants remained as current as possible.

Between May and August 2015 the ACCC sent 5,308 emails inviting individuals to complete the AIC's questionnaire. As some victims provided incomplete or insufficient information that would enable the ACCC to contact them through the post, they were contacted via email. A copy of this email is in *Appendix B*. This information helped them to be confident of the legitimacy of the survey—a particular concern for individuals who had previously experienced online fraud.

The first round of emails was distributed on 15 May 2015 with 4,629 emails being sent to possible victims. Second and third mail-outs were conducted on 2 and 31 July 2015. These resulted in 329 and 350 emails being sent to potential respondents, respectively. Out of the 5,308 emails that were sent, 566 questionnaires were completed—a completion rate of 10.7 percent. Although this rate appears quite low, it is consistent with other similar studies (Ross and Smith 2011).

The same questionnaire used with the victim sample obtained from the ACCC was then administered to a separate independent sample of 1,271 individuals who had subscribed to an online research panel provided by i-Link Research Solutions, a commercial market research provider. It was estimated that at least 200 non-victims would be obtained from a sample of this size. The final non-victim sample size was 321.

To form part of the control group sample, respondents needed to meet the following criteria:

- they had not made a report to the ACCC about goods or services that they had attempted to buy online from overseas since 1 January 2013;
- they were resident in Australia; and
- they had sent money overseas and being completely satisfied with the goods or services received in exchange for that money.

This last criterion could enable victims of online fraud to be included if they were participating in a fraudulent scheme that had yet to be finalised—thus making their victimisation not yet apparent. However, any such individuals would be identifiable through their responses to other questions.

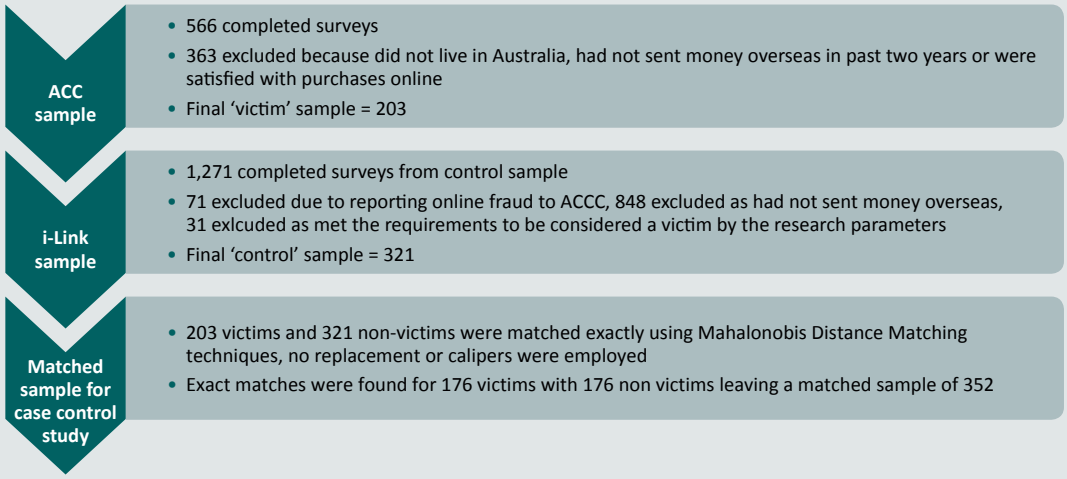
Participants in the i-Link control group were offered a range of rewards by i-Link in exchange for participating in the survey. These rewards form part of i-Link's normal business practices, and were not endorsed by the AIC. Incentives that i-Link participants could select included:

- receipt of instant reward points (accumulated to redeem gifts);
- a chance to win $5,000 quarterly;
- the ability to donate rewards to charity; and
- participation in monthly member competitions/prizes and draws.

Analysis of data

The analysis undertaken for this report was largely descriptive in nature. However, where bivariate analyses were undertaken, appropriate tests to demonstrate statistical significance were also conducted.

Figure 1: Sample creation and responses excluded from analysis to form matched sample (n=352)



Source: AIC Preventing Consumer Fraud Victimisation in Australia 2015 [AIC dataset]

Matched data analysis

In order to determine whether there were differences between victims and non-victims, which might result in some respondents becoming victims of online fraud, it was necessary to select an appropriate comparison group of sufficient size and comparability. This was comprised of a matched group from the samples of victims and non-victims. This type of study was adapted from case-control studies used in epidemiological research, where an outcome (usually a disease) is already known and researchers work backwards to determine how the outcome was reached (Pearce 2016).

The comparison group of non-victims was then matched with victims on:

- gender (exact match);
- age (exact match); and
- highest level of education attained (exact match).

These factors have been demonstrated to have an impact on victimisation (Ross & Smith 2011; Titus & Gover 2001; Whitty 2017). The purpose of matching on these factors was to control their effect on other variables of interest, for example to examine the effect of life events on respondents or online behaviours.

Matching observations were selected using a Mahalanobis distance measure (Tabachnick, Fidell & Osterlind 2001). The case group was selected from among those respondents who were identified by the ACCC as victims of fraud (n=203). Although the current victim sample was drawn from victims who reported to the ACCC's Scamwatch portal, and the non-victim sample matched exactly with the victim sample on age, gender and level of education attained, some differences were observed between demographics of victims in the current sample and victims in the latest Scamwatch study (ACCC 2018): higher proportions of Scamwatch victims were present in the lowest age group, among female victims, and from New South Wales, Queensland and the Northern Territory. These differences were also apparent between the current victims sample and the ACCC's data for 2014 (ACCC 2015).

For each victim in the intervention group, the exact matching non-victim respondent was selected according to the calculated distance measure, subject to the constraints of the variables above. This measure was calculated based on the correlation between two observations, one treated and the other not treated, and then comparing the two across all variables specified in the selection process. The observation within the non-victim group that returned the exact same responses on the three factors measured was then selected as the matched observation within the comparison group. The analysis involved one-to-one exact matching with no replacement and no calliper employed. Exact matches were found for 87 percent of the victims in the intervention group (n=176).

Victim and repeat victim analysis

Respondents were identified as victims from the survey data if they had sent money overseas in the two years prior to completing the survey and they were dissatisfied with what they received in return for sending money. When reviewing these data prior to data matching it was found that a large number of respondents could potentially be considered 'repeat victims' of online fraud. The questionnaire was not specifically designed to gather information on repeat victims; however, owing to the scarcity of research involving repeat victims of online fraud it was felt that further examination of this sub-sample of victims could assist to identify the unique vulnerabilities associated with online fraud. Currently no set definition exists for a repeat victim of online fraud, for example is it a person who sends multiple amounts of money overseas to an online fraud or do they need to be victims of different online frauds? This research used the parameters of sending multiple amounts of money overseas, although the survey did not specifically ask information about scams.

To investigate if there were differences between victims and those who might be considered repeat victims—that is, those who sent money multiple times overseas and were dissatisfied with the outcome—a sample was created from those who indicated they had sent money overseas and specified the amount sent. Respondents who had sent money overseas were asked how much money they sent in the largest transaction in the last two years followed by how much money they had sent in total in the last two years prior to completing the survey. Respondents who had sent a larger total amount in the past two years than the largest transaction in the previous two years (and were dissatisfied with what they received in return for sending this money) were categorised as repeat victims. Those who reported the largest amount sent and the total they had sent overseas in the past two years as the same amount, and were dissatisfied with the outcome, were classified as victims.

Ethical considerations

Several ethical considerations were taken into account when designing this research project. These included consent for respondents, psychological discomfort and confidentiality of victim responses.

The risks associated with consent were minimal, as respondents were taken to have consented by completing the survey. A plain language statement was included at the beginning of the survey to make it clear that participation was voluntary and that respondents were able to end their participation at any stage. Participants were also informed that their survey responses would not be used for official investigations, as all responses were anonymous.

Participants were not asked for any information that would enable them to be identified. The survey findings were only presented as aggregates and the data obtained were stored on a secure server. Care was taken at all times to minimise the risk of data being lost, leaked or accessed without authorisation.

The risk of psychological discomfort associated with this research project was considered to be minimal. However, it was possible that some participants may have become uncomfortable after answering questions about prior victimisation. Given the participants chose to complete the survey and information was provided explaining what the survey was about, it was assumed that they were aware of the more sensitive nature of some of the survey content.

Participants were informed of the availability of counselling services in case they became distressed after recalling their experience of victimisation. The contact details for Lifeline crisis support, SANE Helpline and Grief Line were provided in the introduction to the survey for participants who felt they required additional support.

Limitations of the research design

A number of limitations arose as a result of this research design. First, the sample sizes of the victims and non-victims that were ultimately obtained were relatively small. Accordingly, the results may not be generalisable to the Australian population as a whole. In addition, survey respondents were required to complete the survey online. Therefore, the victim and non-victim samples did not include responses from individuals who may not have had access to a computer.

A second limitation of the research design was that respondents may not have been forthcoming in self-reporting their victimisation experiences. It is also possible that some respondents who were classified as non-victims, were in fact victims of online fraud, but simply did not want to identify themselves as such, or did not realise that they had been victimised. This may be particularly relevant in instances where respondents believed that they might have contributed to their own victimisation, and were embarrassed or ashamed to admit that they played a role in facilitating the fraud.

Thirdly, and as foreshadowed earlier in this report, the definitions that were ultimately used to identify victims and non-victims in this research project could have been refined so as to ensure that the respondents, who were classified as victims, had actually been the victims of an online fraud. To be classified as either a victim or a non-victim, respondents had to have sent money overseas and been dissatisfied with the goods or services received in return for the money sent (the victim sample), or satisfied with the goods or services received in exchange for the money sent (the non-victim sample).

In addition to this, and consistent with the approach adopted by Ross & Smith (2011) in their study about risk factors for advance fee fraud victimisation, sending money overseas was used as an element to define what constituted victimisation for the purpose of this study. Defining victims in such a way means that the characteristics of individuals who were defrauded within Australia after sending money locally or interstate were not included as part of this study. It is, however, likely that most victimisation would have taken place through overseas contacts.

The final limitation related to the fact that the survey did not ask respondents how they rated themselves in relation to certain personal characteristics (such as how likely they were to trust strangers, help those in need, seek opportunities, make impulsive decisions, make intuitive decisions, wait for something due to them, or deal with adverse circumstances) before victimisation compared with after victimisation. Therefore, it was difficult to ascertain if there had been a change in the personal characteristics that certain individuals displayed as a result of the victimisation.

Results

How results are presented

The results are presented in four sections:

- Examining the observed differences between victims and non-victims in their online behaviour—why they sent money overseas, what was the basis of the request they received, if they conducted any research into the undertaking, how much money was sent and how the money was transferred.
- Examining negative life events to determine differences between victims and non-victims in their experiences of these events, and to see if this might be a contributing factor to online fraud victimisation.
- Comparing the victim and non-victim samples in their use of protective factors while using the internet. Protective factors included knowledge about computers and IT, the ability to use computers and associated forms of IT, and what types of computer security respondents used. Personality characteristics were also included in the protective factor questions.
- Exploring victimisation in greater detail. A sample of single-time victims was compared against those identified as repeat victims to examine the effects of victimisation and to see if there were differences between the two types of victims. Findings from the AIC survey were then compared with prior Australian and international research results relating to online fraud victimisation. These comparisons are discussed in greater detail in the *Discussion* section.

Characteristics of the sample

The following tables and figures outline some of the key demographics of the total sample. All survey respondents were aged 15 years and over. Data presenting the characteristics of the sample are presented as descriptive statistics.

Descriptive statistics

Respondents were asked to indicate the age group to which they belonged. Figure 2 shows the age differences between victims and non-victims prior to exact matching. Percentages of victims for each variable are compared with percentages of scam victims who reported losing money to the Scamwatch portal in 2017. Some variation was observed: a higher proportion of Scamwatch victims were aged 34 years and under compared with the current sample; a higher proportion of Scamwatch victims were female than females in the current victim sample; and a higher proportion of Scamwatch respondents in New South Wales, Queensland and the Northern Territory compared with the current sample. These differences were also apparent between the current victims sample and the ACCC's data for 2014 (ACCC 2015). Data on educational and income levels were not available for the Scamwatch victims and so could not be compared with the current sample of victims.

The largest number of victims and non-victims to complete the survey were aged 65 years and over, with 29.6 percent of the victim sample (n=60), and 24.6 percent of non-victims (n=79) falling within this category (see Table 1).

Figure 2: Age of victims and non-victims (%)

Source: AIC Preventing Consumer Fraud Victimisation in Australia 2015 [AIC dataset]

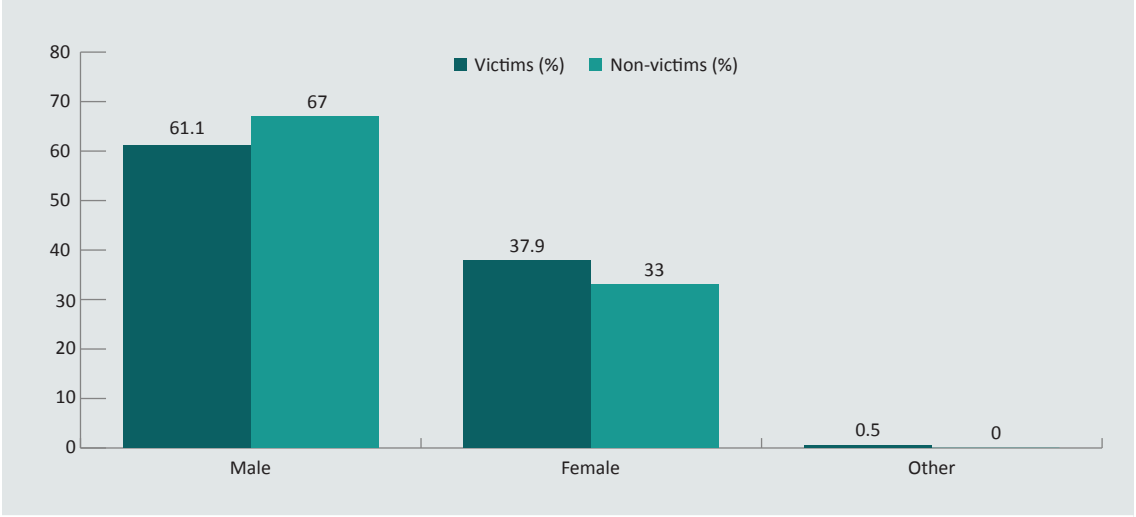
Table 1: Age of matched groups, victims and non-victims (n)

Age group	Victim	Non-victim	Total	Victim %	ACCC (2018)[a]
	n	n	n	%	%
34 and under	20	20	40	11.4	35.1
35–44	24	24	48	13.4	19.0
45–54	42	42	84	23.9	16.9
55–64	35	35	70	20.0	14.3
65 and over	55	55	110	31.3	14.7
Total	176	176	352	100.0	100.0

a: Scam reports with losses in which age was provided (ACCC 2018)
Source: AIC Preventing Consumer Fraud Victimisation in Australia 2015 [AIC dataset]

In response to questions of gender, 61.1 percent of victims indicated they were male (n=124), and 37.9 percent were female (n=77). One victim (0.5%) did not identify as either male or female, and one victim (0.5%) skipped this question. The non-victim sample was also comprised of more males than females with 67 percent (n=215) identifying as male, and 33 percent (n=106) identifying as female (see Figure 3).

Figure 3: Gender of victims and non-victims (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

For the purpose of exact matching, the respondents who failed to provide an answer to questions about their gender were excluded from analysis (Table 2), leaving 222 (111 victims and 111 non-victims) males and 130 females (65 victims and 65 non-victims).

Table 2: Gender of matched groups, victims and non-victims (n)

Gender	Victim	Non-victim	Total	Victim %	ACCC (2018)[a]
	n	n	n	%	%
Male	111	111	222	63.1	49.4
Female	65	65	130	36.9	50.6
Total	176	176	352	100.0	100.0

a: Scam reports with losses in which gender stated (ACCC 2008)
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Respondents were asked to indicate their postcode and usual place of residence. Victims and non-victims were also most likely to reside in New South Wales, with 26.1 percent (n=53) and 25.5 percent (n=82) respectively indicating that this was the state in which they principally lived. No victims indicated they resided in the Northern Territory, with only 1.2 percent of non-victims (n=4) indicating they lived there (see Figure 4).

Figure 4: State/territory of residence of victims and non-victims

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The matched victim and non-victim groups were not matched on place of usual residence and, as can be seen from Table 3, most respondents resided in New South Wales.

Table 3: State/territory place of usual residence of matched groups, victims and non-victims

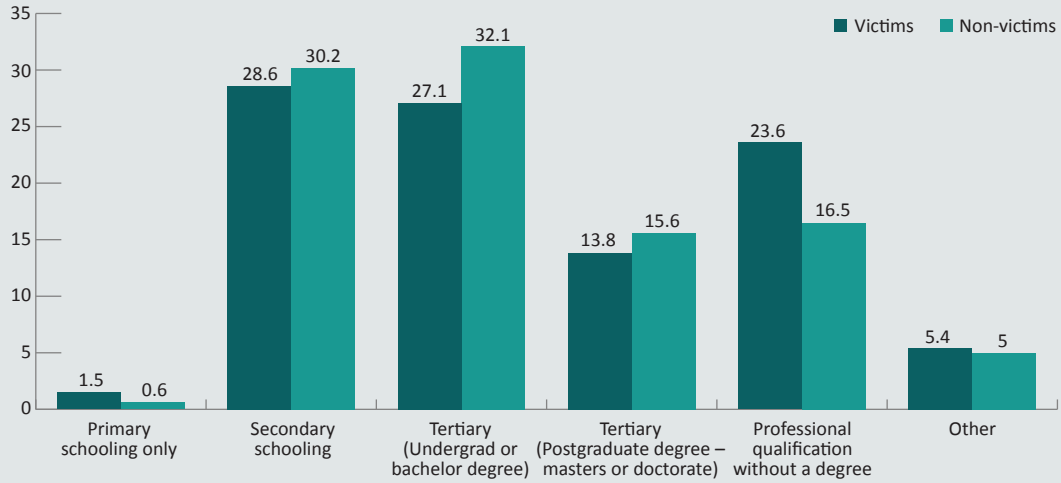
State or territory	Victim	Non-victim	Total	Victim %	ACCC (2018)[a]
	n	n	n	%	%
New South Wales	49	47	96	27.8	30.5
Victoria	40	35	75	22.7	21.6
Queensland	37	38	75	21.0	23.2
Western Australia	20	24	44	11.4	9.6
South Australia	16	17	33	9.1	8.8
Tasmania	8	5	13	4.6	2.4
Australian Capital Territory	6	8	14	3.4	2.9
Northern Territory	0	2	2	0.0	1.0
Total	176	176	352	100.0	100.0

a: Scam reports in which Australian location was stated (ACCC 2018)
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Respondents were asked to indicate the highest level of education that they had completed. When the data were analysed according to whether respondents were victims or non-victims of online fraud, 47.7 percent of non-victims (n=153) had completed a tertiary undergraduate or postgraduate degree, compared with 40.9 percent of victims (n=83). Non-victims were also more likely to have completed secondary school (30.2%, n=97) compared with victims (28.6%, n=58) see Figure 4.

As shown in Figure 5, victims were more likely than non-victims to have completed a professional qualification without a degree, with 23.6 percent (n=48) of victims indicating that this was the case compared with 16.5 percent (n=53) of non-victims.

Figure 5: Educational level of victims and non-victims (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 4 represents the levels of education attained by the matched sample groups. In order to match as many victims with non-victims as possible, the education variable was collapsed into three categories: primary or secondary schooling only; tertiary-level; and trade or professional without a degree.

Table 4: Education of matched groups, victims and non-victims (n)

Educational achievement	Victim	Non-victim	Total
Primary or secondary schooling	53	53	106
Tertiary (undergraduate or postgraduate)	75	75	150
Professional without degree/trade	48	48	96
Total	176	176	352

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Respondents were asked to indicate their individual gross income (before tax had been deducted) from all sources for the last financial year. The largest proportion of victims earned between $37,001 and $80,000 a year (32.5%, n=66), with a similar proportion of non-victims also earning an income within this range (30.8%, n=99). A higher percentage of non-victims than victims earned between $0 and $18,200 a year, with 15.3 percent of non-victims (n=49) reporting an income somewhere within this range, compared with 11.8 percent (n=24) of victims. Approximately three percent of victims (3.0%, n=6) and non-victims (3.1%, n=10) reported an income of $180,001 or more (Figure 6).

Figure 6: Income of victims and non-victims (%)

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 5 outlines the income levels of the matched victim and non-victim groups. The matched sample was not matched on income and accordingly, there are differences between the groups. The largest number of victims and non-victims earned between $37,001 and $80,000. No statistically significant differences were found between the income levels of victims and non-victims ($\chi^2(5, 352)=9.04$, $p=0.11$).

Table 5: Income levels of matched groups, victims and non-victims (n)

Income level	Victim	Non-victim	Total
$0–$18,200	18	31	49
$18,201–$37,000	39	47	86
$37,001–$80,000	55	52	107
$80,001–$180,000	33	29	62
$180,001 and over	6	2	8
I'd rather not say	20	15	35
No response	5	0	5

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Matched sample findings

A case-control study is retrospective. In other words, the outcome is known. In this study, the outcome is online fraud victimisation, and whether certain exposures, such as life events or online behaviours, might contribute to victimisation.

Participants in the victim group (also known as the case group) were matched exactly to participants in the non-victim sample (the control group) according to age, gender and education, using Mahalanobis Distance Matching techniques.

No differences existed between victims and non-victims in their level of IT knowledge. Percentage differences were evident between the matched samples when further analysis of victimisation and the ability to use IT was analysed. However, when the ability to use IT was dichotomised to high/very high level or a very low to moderate level, the difference was not statistically significant.

What makes a victim of online fraud

The questionnaire did not have a specific question that asked if respondents had been victims of online fraud in the previous two years. Rather, respondents were initially asked if they had transferred money overseas in the past two years, for what purpose, and if they were satisfied with the outcome of the undertaking—meaning they received what they thought they were going to get. If a respondent indicated they were dissatisfied with the outcome they were classified as a victim of online fraud.

Online consumer behaviour

Respondents were asked several questions about the purpose behind their decision to send money overseas, and the basis of the request to send money overseas.

These questions were designed to find out what the respondent thought they were sending money for, or to whom they were sending money; how they were approached online; and what, if any, precautions they took in relation to their online activities. By looking at these variables it can be determined if any differences exist between victims of online fraud and people who safely engage in online consumer behaviours.

Purpose of sending money

Respondents were asked to indicate the purpose for which they sent money overseas. Respondents could select more than one response. As shown in Table 6, the main reason for victims and non-victims to send money overseas was to pay for goods and services that they had purchased online, with 81.3 percent of non-victims and 53.2 percent of victims indicating this was the reason for making the payment.

Interestingly, a higher percentage of victims sent money overseas for the purpose of business transactions compared with non-victims, with 20.2 percent of victims indicating this was the case, as opposed to only 8.4 percent of non-victims. A higher percentage of victims also indicated that they sent money overseas to friends they had met online (13.3% of victims compared with 5.9% of non-victims), and to people not personally known to them (36% of victims compared with 1.6% of non-victims).

A number of victims (8.4%, n=17) also indicated they had sent money overseas for reasons other than the options outlined in Table 6. Respondents who answered in this way were asked to specify the purpose for which they sent money overseas. A range of responses was provided, including overseas investments, computer software repairs, schemes involving individuals posing as friends, online dating frauds, and investment fraud.

Table 6: Purpose of sending money overseas—victims and non-victims

Purpose of sending money overseas	Victims		Non-victims	
	n	%	n	%
Paying for goods and services purchased online	108	53.2	261	81.3
Business transactions	41	20.2	27	8.4
Subscriptions to organisations overseas	23	11.3	44	13.7
Sending money to friends I've met online	27	13.3	19	5.9
Sending money to relatives or friends, other than those I've met online	18	8.9	82	25.5
Sending money to people not personally known to you	73	36.0	5	1.6
Donations to charities	12	5.9	26	8.1
Fees, taxes, or charges	11	5.4	16	5.0
Other	17	8.4	6	1.9

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

As there were some distinct differences between victims of online fraud and non-victims and the purposes for which they sent money overseas, some simple bivariate analyses were conducted to see if there were any significant associations between online victimisation and the purpose for which respondents sent money overseas.

Table 7 shows the results of the chi-square tests for why respondents sent money overseas. No significant relationship with victimisation via online fraud was found.

Table 7: Why respondents sent money overseas, matched sample (n)

Purpose	df	χ^2	Significance
Subscription to organisations overseas	1	0.64	0.425
Donations to charities	1	0.72	0.398
Paying fees, taxes or charges	1	0.06	0.080

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 8 shows the relationship between paying for goods and services online and the matched victim/non-victim groups. It was found victims (53%) were less likely to have sent money overseas to pay for goods and services online than non-victims (80%; $\chi^2(1, n=352)=28.04$, $p<0.001$).

Table 8: Contingency table for sending money overseas to pay for goods and services online and victimisation

	Paying for goods and services				Total
	Selected		Not selected		
	n	%	n	%	n
Victim	93	52.8	83	47.2	176
Non-victim	140	79.5	36	20.5	176
Total	223		119		352

***statistically significant at $p<0.001$, Cramér's V=0.2823
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 9 shows the relationship between sending money overseas to pay for a business transaction and being a victim or non-victim. Victims were more likely (18% compared with 9%) than non-victims to send money overseas as a result of a business transaction; ($\chi^2(1, n=352)=7.10$, $p<0.01$).

Table 9: Contingency table for sending money overseas to pay for a business transaction and victimisation

	Business transactions				Total
	Selected		Not selected		
	n	%	n	%	n
Victim	93	52.8	83	47.2	176
Non-victim	140	79.5	36	20.5	176
Total	223		119		352

**statistically significant at $p<0.01$, Cramér's V=0.1420
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 10 indicates victims are more likely than non-victims (13% compared with 3%) to send money overseas when requested by someone they met online ($\chi^2(1, n=352)=9.93$, $p<0.01$).

Table 10: Contingency table for sending money overseas to friends met online and victimisation

	Sending money to online friends				Total
	Selected		Not selected		
	n	%	n	%	n
Victim	22	12.5	154	87.5	176
Non-victim	6	3.4	170	96.6	176
Total	28		324		352

**statistically significant at $p<0.01$, Cramér's V=0.17
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Non-victims on the other hand were more likely to send money overseas to friends or family members they met offline (26% compared with 9% of victims; $\chi^2(1, n=352)=19.06$, $p<0.001$). See Table 11.

Table 11: Contingency table for sending money overseas to friends or relatives or persons other than those met online and victimisation

	Sending money to friends or family				Total
	Selected		Not selected		
	n	%	n	%	n
Victim	15	8.5	161	91.5	176
Non-victim	46	26.1	130	73.9	176
Total	61		291		352

***statistically significant at $p<0.001$, Cramér's V=-0.23
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Finally, as shown in Table 12, victims were substantially more likely to send money to people they did not personally know than non-victims (38% of victims compared with 1% of non-victims). This association between victimisation and sending money overseas to people not personally known to them was a strong association ($\chi^2(1\ n=352)=77.88$, $p<0.001$, Cramér's V=0.47).

Table 12: Contingency table for sending money overseas to people not personally known to you and victimisation

	Sending money to online friends				Total
	Selected		Not selected		
	n	%	n	%	n
Victim	66	37.5	110	62.5	176
Non-victim	1	0.6	175	99.4	176
Total	67		285		352

***statistically significant at $p<0.001$, Cramér's V=0.47
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Basis for sending money

Respondents were asked about the basis of the request they received to send money overseas, such as from an online shopping site or participation in a lottery or competition. These questions were devised to see if the person making the request for money was using well-known fraudulent techniques or if there was a legitimate purpose behind the request to send money.

Participants who specified that they had sent money overseas for 'other reasons' were asked to outline what these reasons were. Just over 22 percent of non-victims said they sent money overseas for the purpose of payments/gifts to family members and business expenses. Similarly, almost 20 percent of victims also specified 'other reasons' for why they sent money overseas. These 'other reasons' included payment for dating certificates; fees to cover the cost of having their computer fixed; and fees for notaries or other legal fees.

A higher number of victims than non-victims identified reasons for sending money overseas that have traditionally been associated with online fraud (Table 13). For example, 22 percent of victims identified the opportunity to gain a financial reward as the basis for why they sent money overseas compared with less than one percent of non-victims. Also, 15.3 percent of victims sent money overseas to assist someone they had met online compared with only three percent of non-victims.

Table 13: Basis of request to send money overseas—matched victim/non-victim sample

Basis of request to send money	Victims		Non-victims		Total
	n	%	n	%	n
A payment in connection with an online purchase or sale of goods or services	77	43.8	119	67.6	196
An offer of a job or acting as an employee or consultant	4	2.3	1	0.6	5
The opportunity to gain a financial reward	39	22.2	1	0.6	40
Assisting another person or agency with the distribution of charitable funds	1	06	2	1.1	3
Participating in a lottery or other prize competition	14	8.0	1	0.6	15
Helping someone to recover money that was owed to them	8	4.5	2	1.1	10
Assisting a foreign dignitary	2	1.1	0	0	2
Refund of bank fees, taxes, or government benefits or an over-invoiced contract	2	1.1	0	0	2
Unclaimed bank account	5	2.8	1	0.6	6
Providing money to help someone I'd met online	27	15.3	6	3.4	33
Cleaning 'black cash'	0	0.0	0	0.0	0
Transfer of funds from deceased estate	5	2.8	5	2.8	10
Other basis of request	37	21.0	46	26.1	83

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Analyses were conducted to determine if there were any significant relationships between online fraud victimisation and the basis of the request made to respondents who transferred money overseas. A significant association was found between non-victims and sending money overseas to pay for online purchases or the sale of goods or services. Non-victims were more likely than victims (68 percent, compared with 44 percent) to have sent money overseas based on that premise, ($\chi^2(1,352)=20.3$, $p<0.001$, Cramér's V=-0.24).

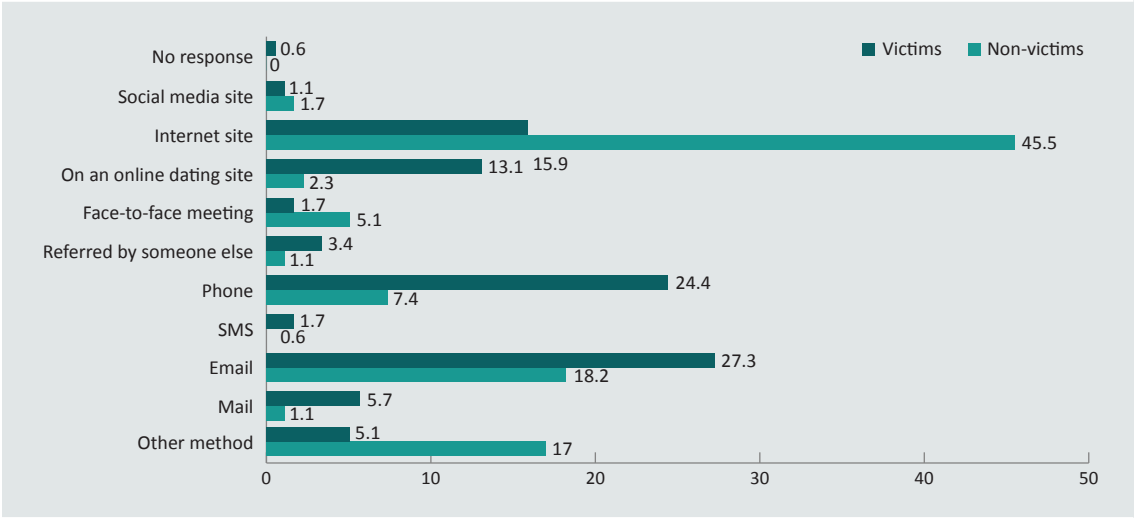
Victims were more likely than non-victims to have sent money overseas based on a request that involved the opportunity to gain a financial reward (22% of victims compared with 1% of non-victims), ($\chi^2(1,352)=40.73$, $p<0.001$, Cramér's V=0.34). This association between the opportunity to gain a financial reward and online victimisation was moderately strong.

A relationship was also found to exist between victimisation and sending money overseas to participate in a lottery or some other prize competition. Victims were more likely than non-victims to have reported this as the basis of the request for transferring money overseas. Due to the low number of respondents who sent money as a result of this request (n=15) a Fisher's exact test was conducted ($p<0.01$).

How contact was made

Participants were asked to indicate how contact was first established with the recipient of the largest sum of money that they had sent overseas in the last two years. Most non-victims identified internet sites as the method that they used initially to contact the recipients of overseas payments that they made (45.5%, n=80). In contrast to this, victims identified email (27.3%, n=48) and phone (24.4%, n=43) as the two most common ways in which they initially made contact with the recipients of the overseas payments that they made (see Figure 7).

Figure 7: Method used to establish first contact with recipient of overseas payment (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Researching the undertaking prior to sending money overseas

Participants were asked whether they undertook any research on the internet or elsewhere about the person or organisation with whom they were dealing or the proposal involved. With respect to whether victims and non-victims conducted any research about the entity or proposal prior to actually sending money overseas, more than 50 percent of victims (52.3%) indicated that they had researched the proposal or entity before they decided to send money, compared with 33 percent of non-victims. Participants who had undertaken research on the entity or proposal prior to sending money were asked to specify the kind of information they found or received. Internet research was the most common way in which information about the entity or proposal was obtained, with Google, review feedback and seller ratings on sites such as eBay mentioned by a number of respondents.

Just over 47 percent of victims (47.7%) indicated that they did not conduct any research prior to sending money overseas, compared with 67 percent of non-victims (Table 14).

Table 14: Research conducted prior to sending money overseas, victims and non-victims

Research conducted	Victims		Non-victims	
	n	%	n	%
Yes	92	52.3	58	33.0
No	84	47.7	118	67.1
Total	176		176	

***statistically significant at $p<0.001$
Note: Due to rounding, percentages may not total 100
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The finding that victims of online fraud were statistically more likely to research the undertaking prior to sending money was initially confusing ($\chi^2(1,352)=13.43$, $p<0.001$). It is reasonable to assume if you research the opportunity you will find it may be fraudulent and not become a victim. However, when the types of research conducted were reviewed there were differences between victims and non-victims. Ninety-two victims provided details of the type of research they conducted prior to sending money overseas. Of those, 23 percent (n=21), reported that their research involved looking at the website of the business or the person they were dealing with. For example, one respondent said '(I) read all the fine print on the web page.' Another victim indicated that they 'looked at their website which looked legitimate'. In contrast to this, non-victims indicated that their research involved '(I) Googled reviews' and 'reviews and feedback from users.' More non-victims (n=15) used internationally well-known online shopping sites. In addition, non-victims sought feedback about the business and product from sites other than the organisation's website.

Amount of money sent overseas

Respondents were asked to specify how much money they had sent overseas altogether during the last two years in relation to the particular undertaking or proposal. For ease of analysis the amounts of money that were sent were placed in categories (see Table 15). Almost all of the non-victims (94.4%) sent between $0 and $5,000 overseas during the last two years, compared with 64 percent of victims.

Table 15: Total amount of money sent overseas during the last two years, victims and non-victims

Amount sent	Victims		Non-victims	
	n	%	n	%
$0–$5,000	130	64.0	303	94.4
$5001–$10,000	19	9.4	9	2.8
$10,001–$20,000	21	10.3	4	1.2
$20,001–$40,000	13	6.4	3	0.9
$40,001–$80,000	6	3.0	1	0.3
$80,001–$160,000	8	3.9	1	0.3
$160,001–$320,000	2	1.0	0	0.0
> $320,001	4	2.0	0	0.0

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Victims appeared to have sent more money overseas during the last two years than non-victims, with 10.3 percent of victims sending between $10,001 and $20,000, 9.4 percent sending between $5,001 and $10,000, and 6.4 percent sending between $20,001 and $40,000. In contrast to this, only 2.8 percent of non-victims sent between $5,001 and $10,000 and 1.2 percent sent between $10,001 and $20,000. Less than two percent of non-victims sent between $20,001 and $160,000. The amounts of money sent overseas by victims and non-victims are explored in more detail in the matched data section (Figure 8).

Figure 8: Largest amount of money sent overseas in the previous two years by victims and non-victims matched groups (n)

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

As shown in Table 15, there was a difference in the amounts of money sent overseas by victims compared with non-victims. The matched data were consistent with this, with the largest amount of money sent overseas by victims being higher than that sent by non-victims (Figure 7). As the data were exactly matched, it was not appropriate to transform the data as this may have caused some of the matches to be dropped or changed. Using the Mann-Whitney U test was the best equivalent of the t-test under these circumstances.

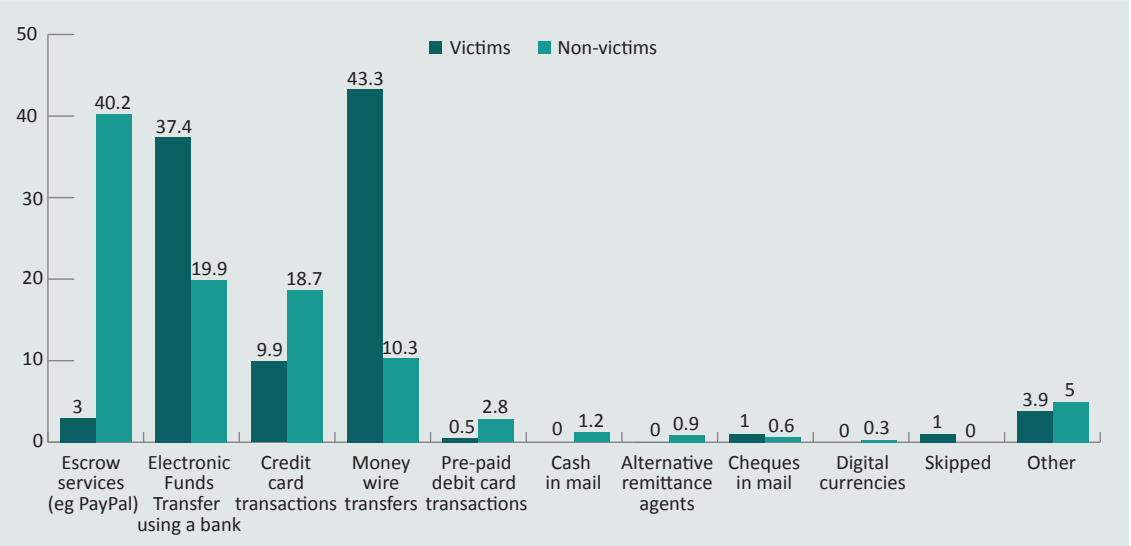
The Mann-Whitney U test examined if the observed differences in the largest amount of money sent by victims and non-victims were statistically significant. This non-parametric test was used because the dependent variable of how much money was sent overseas in the largest transaction was not normally distributed. The distribution was positively skewed with more respondents of each group sending lower amounts of money overseas. The test found that non-victims sent significantly less money overseas than victims of online fraud ($z=-9.582$, $p<0.01$, $n=352$). When looking at the differences between victims and non-victims and the total amount sent in the past two years, the Mann-Whitney U test found non-victims sent significantly less money in total overseas than victims ($z=-7.392$, $p<0.001$, $n=352$).

How money was transferred overseas

Participants were asked which funds transfer method they used for the largest funds transfer overseas in the last two years. The most common method victims used was money wire transfer (43.3%), followed by electronic funds transfer using a bank (37.4%), and credit card transactions (9.9%).

By contrast, only 10.3 percent of non-victims indicated that they used money wire transfers to transfer funds overseas, with the most common funds transfer method for non-victims being escrow services such as PayPal (40.2%). This was followed by electronic funds transfer using a bank (19.9%) and credit card transactions (18.7%). See Figure 9.

Figure 9: Funds transfer method used by victims and non-victims (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

When the matched samples were examined, the differences in how victims and non-victims transferred money overseas were found to be statistically significant. Victims were more likely to use electronic funds transfers, or direct credit, than non-victims (37% compared with 20% of non-victims); or use money wire transfers such as companies like Western Union or TravelEx, than non-victims (43% compared with 10% of non-victims). Conversely non-victims were more likely to use credit card transactions (20% of non-victims compared with 10% of victims), or use escrow services such as PayPal, than victims—some 41 percent of non-victims compared with three percent of non-victims ($\chi^2(10, n=352)=118.58$, $p<0.001$).

Life events and personal characteristics of participants

Participants were asked questions about themselves and events that may have happened to them in the past that possibly could have had some effect on their becoming victims of online fraud. By comparing the characteristics of victims and non-victims, it was hoped that behavioural patterns or lifestyle characteristics could be identified that might assist in identifying individuals who may be susceptible to becoming victims of online fraud in the future.

Lifestyle events experienced by victims and non-victims

Participants were asked a number of questions about life events that they had experienced within the last five years. As was the case in relation to the characteristics discussed above, one of the limitations of the survey instrument used in this research was the fact that it did not ask participants whether these events took place prior to, or after, the participants sent money overseas.

Table 16: Victim and non-victim experiences with life events (n)						
Life event	Victims			Non-victims		
	Yes	No	I'd rather not say	Yes	No	I'd rather not say
Ever declared bankrupt	18	156	2	15	159	2
In the last five years a close family member or friend died	97	73	6	84	88	4
In the last five years suffered depression	64	101	5	56	115	5
In the last five years lost job	42	127	7	32	140	4
In the last five years being diagnosed with a serious illness	28	142	6	28	140	8
In the last five years being a victim of a serious accident	7	167	2	2	170	4
In the last five years marriage or other close personal relationship breakdown	36	135	5	19	153	4
In the last five years victim of a serious crime (eg theft, burglary, assault or sexual≈assault)	18	156	2	15	159	2

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

A series of chi-square tests were performed to determine if there were an association between certain life events and victimisation. Only one statistically significant relationship was found to exist between any of the variables that were examined, and victimisation. Table 16 presents the number of respondents who had experienced those events, those who had not, and the small number who would prefer not to say. An association was found between victims and respondents who had experienced either their marriage or another close personal relationship breaking up in the last five years (Fisher's exact $p<0.05$).

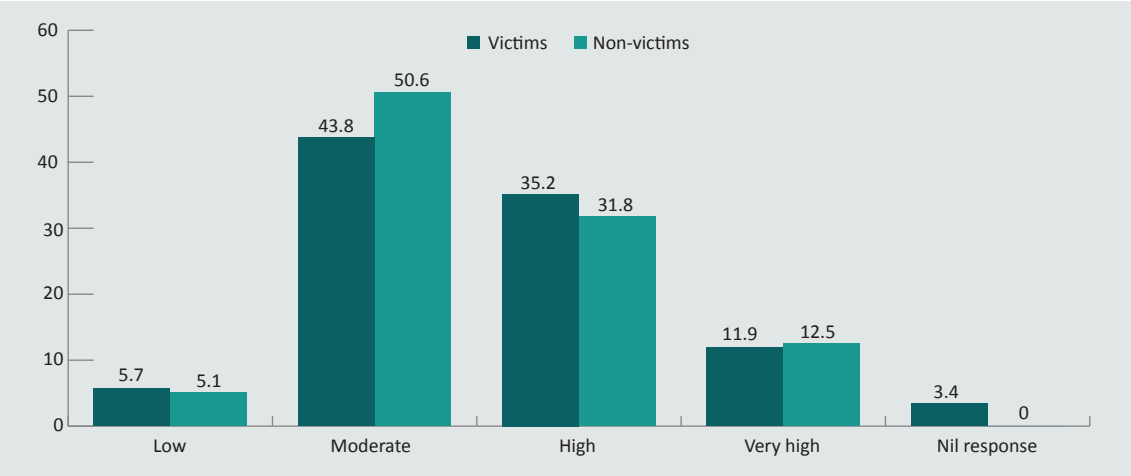
Preventive factors used by victims and non-victims with online activities

The following section explores a number of variables to determine if there were differences in the ways that victims of online fraud engaged in consumer activity online compared with non-victims. The online activities that were examined included: level of understanding about computers and computer security; types of computer security that were used by respondents while online; and how much time respondents spent online. Other variables that were examined included: why respondents sent money overseas; the basis of the request they received prior to sending the money; the reason they sent the largest sum of money in the two years prior to completing the survey; if the respondents conducted any research about the undertaking prior to sending money; the amounts of money sent overseas by victims and non-victims; and how they sent the money overseas.

Computer security and usage

All respondents were asked how they would rate their level of knowledge and their ability to use computers or other forms of IT on a Likert scale ranging from 'very low' to 'very high'. As Figures 10 and 11 demonstrate, victims and non-victims appeared to rate themselves quite similarly when it came to their knowledge of and ability to use computers and IT. For instance, more than 40 percent of victims (47.1%, n=83) and non-victims (44.3%, n=81) rated their level of knowledge of this technology as 'high' or 'very high,' and only a slightly higher percentage of non-victims (50.6%, n=89) rated their level of knowledge as 'moderate' compared with victims (43.8%, n=77). See Figure 10. No significant relationship was found to exist between respondents' knowledge of computers and IT and online fraud victimisation.

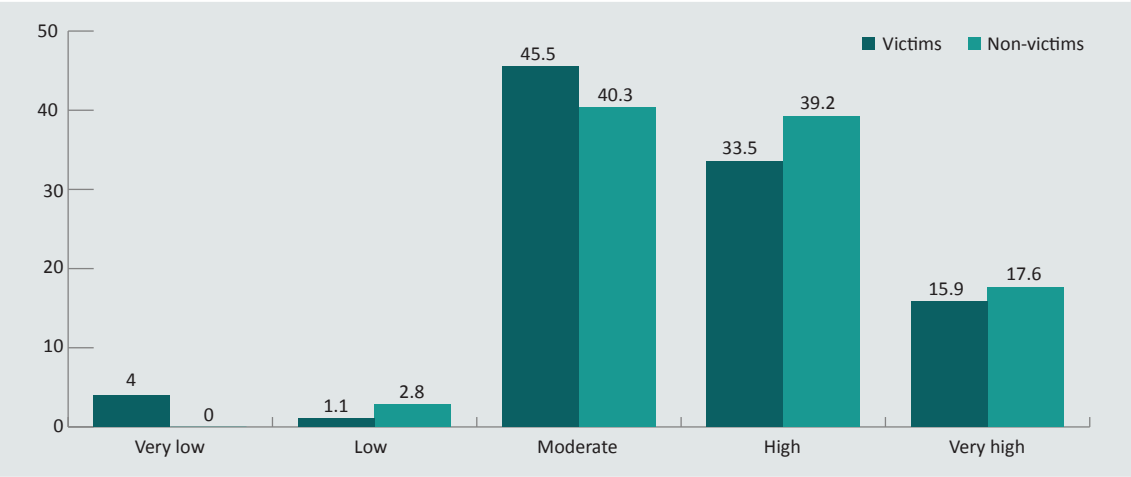
Figure 10: Victims' and non-victims' level of knowledge about computers and Information Technology (IT)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

With respect to the ability to use computers and IT, 56.8 percent of non-victims (n=100) rated their ability as 'high' or 'very high', compared with 49.4 percent of victims (n=87). See Figure 11. There was no statistically significant difference between victims and non-victims in their ability to use computers (p=0.05). Five percent of victims (n=9) and three percent of non-victims (n=5) rated their ability to use computers as 'low' or 'very low'.

Figure 11: Victims' and non-victims' ability to use computers and IT



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Respondents were asked how many hours each week they spent using the internet for work and personal use, including email. Most non-victims (80.6%, n=142) used the internet for 10 or more hours a week. Differences were identified in the number of hours that victims and non-victims spent using the internet each week, with non-victims spending more time each week accessing the internet than victims (see Figure 12; $\chi^2(5, n=352)=22.80$, $p<0.001$, Cramér's V=0.25).

Figure 12: Hours spent by victims and non-victims on the internet each week (%)

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 17 presents the findings for how much time respondents spent using the internet when the victim and non-victim samples were exactly matched on age, gender and education.

Table 17: Hours spent on the internet each week, matched sample of victims and non-victims (n)

Hours spent using internet	Non-victim	Victim	Total
1 or less hours	0	3	3
2–4 hours	12	32	44
5–9 hours	22	36	58
10–19 hours	62	50	112
20 or more hours	80	54	134
Answer not provided	0	1	1
Total	176	176	352

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The findings indicate some differences between victims and non-victims and the number of hours spent using the internet. Given that frequency of online behaviour may have an impact on victimisation, further analyses were conducted. Internet use was dichotomised to either more than 10 hours a week or less than 10 hours a week. A statistically significant relationship was found between time spent using the internet and victimisation. A higher proportion of non-victims spent 10 hours or more each week using the internet than victims, with 81 percent of non-victims spending this amount of time online each week compared with 59 percent of victims ($\chi^2(1,352)=19.49$, $p<0.001$). The strength of the association, using Cramér's V, was only moderate (V=0.24).

This finding may suggest experience and familiarity can protect against victimisation, whereas people spending less time on the internet may be less familiar and therefore more prone to risky behaviour or not verifying vendors.

Respondents were asked about the computer security measures that they used and were able to select more than one security measure. As indicated in Table 18, passwords were the most common measure used by both victims (88.7%) and non-victims (88.5%) to secure computers. Also, there was very little difference in the percentage of victims and non-victims who used anti-virus software and anti-spam filters, with 86.9 percent of non-victims and 86.2 percent of victims indicating that they used anti-virus software and 59.8 percent of non-victims and 59.6 percent of victims indicating that they used anti-spam filters.

Table 18: Computer security measures used by victims and non-victims

Computer security measure	Victims		Non-victims	
	n	%	n	%
Using passwords to logon	180	88.7	284	88.5
Physically securing computers or wireless devices	47	23.2	69	21.5
Encryption of data	20	9.9	48	15.0
Anti-spam filters	121	59.6	192	59.8
Anti-virus software	175	86.2	279	86.9
Anti-spyware software	105	51.8	202	62.9
Anti-phishing software	68	33.5	143	44.5
Internet content/image filtering or monitoring	30	14.8	82	25.5
Firewall	138	68.0	232	72.3
Other	3	1.5	2	0.6
None	1	0.5	6	1.9
I don't know	9	4.4	7	2.2

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The various types of computer and information and communications technology (ICT) security used were analysed using the matched victim/non-victim sample to determine if there were any significant differences between how people secured their computers that might indicate an increased chance of online fraud victimisation. No significant relationships were found between victimisation and the use of passwords, physically securing computers or wireless devices, encryption of data, anti-spam filters, anti-virus software and the use of firewalls. Very few respondents reported using no computer security measures.

Three types of computer and security were found to be statistically related to victimisation (Table 19). Non-victims were more likely than victims to use anti-spyware software ($\chi^2(1,352)=6.769$, $p<0.01$, Cramér's V=0.1387); anti-phishing software ($\chi^2(1,352)=7.425$, $p<0.01$, Cramér's V=0.1449), and content and imaging filtering ($\chi^2(1,352)=7.214$, $p<0.01$, Cramér's V=0.1423). None of the effect sizes were very large, indicating a weak association between the specific type of computer security and victimisation.

Table 19: Contingency table of victim and non-victim use of computer security measures

Type of computer security	Victims n (%)		Non-victims n (%)		χ^2
	Selected	Not selected	Selected	Not selected	
Anti-spyware software	92 (52.3)	84 (47.7)	116** (65.9)	60 (34.1)	6.77
Anti-phishing software	58 (33.0)	118 (67.1)	83** (47.2)	93 (52.8)	7.43
Content and image filtering	25 (14.2)	151 (85.8)	45** (25.6)	131 (74.4)	7.21

**statistically significant at $p<0.01$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Personal characteristics of victims compared with non-victims

The questionnaire contained seven questions asking participants about their personality traits. Participants were asked to rate their likelihood of behaving in certain ways on a scale ranging from 'very unlikely' to 'very likely'. The characteristics of victims and non-victims were explored in more detail. The personality characteristics are not from a set psychological scale but are traits that have been linked to psychological factors that may make some people more vulnerable to fraudulent schemes.

However, the survey instrument did not ask respondents how they rated themselves in relation to certain personal characteristics before victimisation compared with after victimisation. This meant that analysis could not be conducted to ascertain if there had been a change in the personal characteristics that certain individuals displayed as a result of victimisation. Table 20 shows the descriptive statistics of victim and non-victim responses to the questions. A number of differences were evident between the two groups (except for the characteristic 'deal with adverse circumstances'), and were included in the multivariate analyses below.

Table 20: Personal characteristics of victims and non-victims					
Characteristic	**Very unlikely**	**Unlikely**	**Neutral**	**Likely**	**Very likely**
Trust strangers* **					
Victims	79 (44.9%)	47 (26.7%)	33 (18.8%)	15 (8.5%)	2 (1.1%)
Non-victims	42 (23.9%)	48 (27.3%)	66 (37.5%)	17 (9.7%)	3 (1.7%)
Help those in need **					
Victims	24 (13.6%)	26 (14.8%)	44 (25.0%)	64 (36.4%)	18 (10.2%)
Non-victims	7 (4.0%)	12 (6.8%)	56 (31.8%)	71 (40.3%)	30 (17.0%)
Seek opportunities* **					
Victims	30 (17.0%)	42 (23.9%)	47 (26.7%)	48 (27.3%)	9 (5.1%)
Non-victims	11 (6.3%)	16 (9.1%)	77 (43.8%)	61 (34.7%)	11 (6.3%)
Make impulsive decisions* **					
Victims	59 (33.5%)	63 (35.8%)	31 (17.6%)	20 (11.4%)	3 (1.7%)
Non-victims	27 (15.3%)	60 (34.1%)	54 (30.7%)	32 (18.2%)	3 (1.7%)
Make intuitive decisions* **					
Victims	30 (17.0%)	34 (19.3%)	59 (33.5%)	43 (24.4%)	10 (5.9%)
Non-victims	9 (5.1%)	10 (5.9%)	56 (31.8%)	89 (50.6%)	12 (6.8%)
Wait for something due to me* **					
Victims	36 (20.5%)	37 (21.0%)	71 (40.3%)	29 (16.5%)	3 (1.7%)
Non-victims	8 (4.5%)	16 (9.1%)	80 (45.5%)	65 (36.9%)	7 (4.0%)
Deal with adverse circumstances					
Victims	21 (11.9%)	12 (6.8%)	65 (36.9%)	58 (33.0%)	20 (11.4%)
Non-victims	9 (5.1%)	8 (4.5%)	61 (34.7%)	76 (43.2%)	22 (12.5%)

***statistically significant at the $p<0.001$ level, **statistically significant at the $p<0.01$ level
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Based on the prior research about vulnerability to fraud victimisation discussed in the introduction to this report, further analyses examined if victimisation through online fraud could be predicted through hours spent using the internet each week, the number of computer security measures used, and personality traits of trusting strangers, helping those in need, making impulsive decisions, relationship status and the method used to send money overseas. The variables around the type of computer security measures used were collapsed into an 'advanced computer security' variable which included the following categories: encryption of data, anti-spam filters, anti-virus software, anti-spy software, anti-phishing software and internet content/imaging filtering or monitoring. Unlike passwords or firewalls, these categories of computer security are not standard with most computers and internet service providers, and involve a level of technical understanding above physically securing a computer or wireless device.

A dummy dichotomous variable was created for 'how money was sent overseas' to include if money was sent overseas via electronic transfer or via money wire transfer (as victims were found to be more likely to use these methods of payment than non-victims) versus not using that method. There were few significant associations with life events. However, it was found that victims were more likely to have suffered a relationship breakdown than non-victims. Therefore relationship breakdown in the past five years (yes/no) was included in the model.

The analysis involved logistic regression where the predictor variable was a binary outcome of either victim or non-victim. The primary hypothesis was that greater levels of computer security would decrease the likelihood of online fraud victimisation. It was also hypothesised that the more time a person spent using the internet, the less likely it would be that they would become a victim of online fraud, since familiarity with the internet and searching websites would act as a preventative factor. The variables age, gender and education were not included in the model as they were the variables where the victim and non-victim groups were exactly matched.

The overall model (see Table 21) was statistically significant in predicting factors that would increase online fraud victimisation ($\chi^2(12,352)=131.25$, $p<0.001$). The model predicted factors impacting online fraud victimisation better than no model at all, with an area under the Receiver Operator Curve (ROC) of 0.83. An acceptable range and the variance explained by the model was: Nagelkerke=0.419. Importantly, the main hypothesis that respondents with greater levels of computer security would be less likely to be victims of online fraud was not supported. However, the hypothesis that greater familiarity with online activities would result in a reduced likelihood of victimisation was supported.

The only life event which was found to have a significant association with victimisation was whether or not a relationship had broken down. However, when included in the model this variable was not statistically significant. The model also showed victims were more likely to use methods such as money wire transfers and electronic funds transfers to send money to people who turn out to be scammers.

Table 21: Logistic regression: predictors of online fraud victimisation versus not being a victim

Variable	Odds ratio	SE	Wald (z statistic)	*p*-value
Advanced computer security	0.891	0.063	-1.64	0.102
Greater than 10 hours on internet	0.356	0.093	-3.94	0.000
Trust strangers 1—unlikely	0.679	0.212	-1.24	0.216
Trust strangers 2—neutral	0.385	0.131	-2.82	0.005
Trust strangers 3—likely	0.662	0.303	-0.90	0.367
Trust strangers 4—very likely	0.612	0.608	-0.47	0.622
Make impulsive decisions—1 unlikely	0.705	0.235	-1.05	0.295
Make impulsive decisions—2 neutral	0.458	0.174	-2.06	0.039
Make impulsive decisions—3 likely	0.409	0.174	-2.11	0.035

Table 21: Logistic regression: predictors of online fraud victimisation versus not being a victim

Variable	Odds ratio	SE	Wald (z statistic)	*p*-value
Make impulsive decisions—4 very likely	0.657	0.583	-2.11	0.636
Relationship breakdown had occurred—1	1.510	0.383	1.08	0.282
Money transferred via electronic funds transfer or money wire transfer—1	8.870	0.273	7.99	0.000
Constant	6.859	2.468	5.35	0.000

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Victimisation and repeat victimisation

Respondents who were identified as victims of online fraud were asked several additional questions to understand the effect and consequences of online fraud. These respondents were also asked if they had reported the online fraud to anyone, such as a government agency, or a support organisation or friend/family member.

Although the questionnaire was not designed to investigate repeat victimisation via online fraud, after analysing the data pertaining to victims, it was found that among the 203 victims was a group of 'repeat victims'. These repeat victims had transferred multiple amounts of money overseas and had reported they were unhappy with the outcome that resulted in return for sending the money. There were 58 respondents identified as repeat victims, 29 percent of the victim sample.

Analyses were undertaken to determine if there were differences in online behaviour between one-off victims of online fraud and those who were repeat victims.

Characteristics of victims and repeat victims

The characteristics of victims and repeat victims were explored in greater detail. Chi-square tests, which test the assumption that frequencies observed in each cell are obtained by chance, were used for categorical variables. Table 22 shows the results of the chi-square tests for those variables found not to have a significant relationship with repeat victimisation in the previous two years.

Table 22: Variables that did not have a significant relationship with repeat victimisation/ victimisation in the past two years (n=151)

Variable	df	χ^2	*Significance*
Age	6	2.50	0.93
Gender	2	0.56	0.756
Education	5	3.82	0.576

Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

A significant relationship was found between the individual gross income category and if a victim was a repeat victim or a one-time victim in the past two years ($\chi^2(5,151)=13.04$, $p<0.05$; see Table 23). These results indicate that those in the highest income category ($180,001 and over) were more likely to experience repeat victimisation than respondents earning less money (8% repeat victims vs 1% one-time victims). Respondents who preferred not to indicate their income were less likely to be repeat victims (16% one-time victims vs 3% repeat victims). This may reflect a reluctance to divulge their personal information, which may translate to a reduced willingness to engage in potentially risky behaviour online.

Table 23: Contingency table for repeat victimisation/victimisation via online fraud in the past two years and individual gross income

Income category	Victims		Repeat victims		Total
	n	%	n	%	n
$0–$18,200	10	9.7	10	17.2	20
$18,201–$37,000	23	22.3	12	20.7	35
$37,001–$80,000	30	29.1	19	32.8	49
$80,001–$180,000	23	22.3	10	17.2	33
$180,001 and over	1	41.0	5*	8.6	6
I'd rather not say	16*	15.5	2	3.5	18
Total	103		58		161

*statistically significant at $p<0.05$
Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

Purpose for sending money overseas

To examine if there were differences in the purposes behind repeat victims and one-off victims sending money overseas, bivariate analyses were conducted using the victim/repeat victim sample.

Several categories showed no statistical relationship between repeat victimisation and the purposes for sending money. They were:

- paying for goods and services purchased online;
- business transactions;
- sending money to relatives or friends, other than those I've met online;
- donations to charities;
- fees, taxes or charges; and
- other purposes.

As shown in Table 24 a significant relationship was found between sending money overseas for subscriptions to overseas organisations and repeat victimisation, ($\chi^2(1,161)=4.13$, $p<0.05$, Cramér's V=0.16). Repeat victims were more likely (16% compared with 6% of victims) than one-time only victims to have indicated the purpose of sending money overseas was to pay for overseas subscriptions, but this association was relatively weak.

Table 24: Contingency table for sending money overseas for subscriptions to organisations overseas and repeat victimisation

	Sending money for subscriptions				Total
	Selected		Not selected		
	n	%	n	%	
Repeat victim	9*	15.5	49	84.5	58
Victim	6	5.8	97	94.2	103
Total	15		146		161

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 25 shows a significant relationship between repeat victimisation and respondents sending money overseas to friends they had met online ($\chi^2(1,161)=5.70$, $p<0.05$, Cramér's V=0.19). Repeat victims were more likely than single-time victims to have sent money overseas to friends they had met online (21% compared with 8%).

Table 25: Contingency table for sending money overseas to friends respondent had met online and repeat victimisation

	Sending money to friends met online				Total
	Selected		Not selected		
	n	%	n	%	
Repeat victim	12*	20.7	46	79.3	58
Victim	8	7.8	95	92.2	103
Total	20		141		161

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Lastly, a significant relationship was found between repeat victims and those who sent money to people not personally known to them ($\chi^2(1,161)=4.84$, $p<0.05$, Cramér's V=0.17). Although the association was weak, it was found that repeat victims were more likely (43% compared with 26% of other victims) to send money to people not personally known to them who were based overseas (Table 26).

Table 26: Contingency table for sending money overseas to people not personally known to them and repeat victimisation

	Sending money to friends met online				Total
	Selected		Not selected		
	n	%	n	%	
Repeat victim	12*	20.7	46	79.3	58
Victim	8	7.8	95	92.2	103
Total	20		141		161

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The basis of sending money

The basis of the request for sending money overseas was examined using the one-time victim and repeat victim sample. When these variables were analysed a few significant differences were found. No relationship was found between repeat victims and the following basis of requests:

- an offer of a job or acting as an employee or consultant;
- the opportunity to gain a financial reward;
- assisting another person or agency with the distribution of charitable funds;
- participating in a lottery or other prize competition;
- helping someone to recover money that was owed to them;
- assisting a foreign dignitary;
- refund of bank fees, taxes or government benefits or an over-invoiced contract;
- unclaimed bank account;
- cleaning 'black cash';
- transferring funds from deceased estate; and
- other requests.

When looking at the victim and non-victim samples above, non-victims were more likely to send money overseas as a result of purchasing goods and services overseas. However, when the same variable was analysed with the one-off and repeat victim sample, a difference was found (Table 27). Repeat victims were less likely than other victims to have sent money overseas in connection with online purchases of goods and services—34 percent of repeat victims compared with 53 percent of single event victims ($\chi^2(1,161)=5.34$, $p<0.05$).

Table 27: Contingency table for sending money overseas on the basis of purchasing goods and services online and repeat victimisation

	Basis of request: purchasing goods and/or services online				Total
	Selected		Not selected		
	n	%	n	%	
Repeat victim	20	34.5	38	65.5	58
Victim	55*	53.4	48	46.6	103
Total	75		86		161

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The findings from Table 28 indicate that repeat victims were twice as likely to send money to help someone they had met online than other victims (22% of repeat victims compared with 11% of victims, $\chi^2(1,161)=4.03$, $p<0.05$), although the association between repeat victims and providing money to help someone they had met online was weak, with a Cramér's V of 0.16.

Table 28: Contingency table for sending money overseas on the basis of helping someone the respondent had met online and repeat victimisation

	Basis of request: sending money to help someone met online				Total
	Selected		Not selected		
	n	%	n	%	n
Repeat victim	13*	22.4	45	77.6	58
Victim	11	10.7	92	89.3	103
Total	24		137		161

*statistically significant at $p<0.05$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Amount of money sent overseas

As there were significant differences found between victims and non-victims in the total amounts of money sent overseas and in the largest amount—the amount of money sent overseas by repeat victims was also examined to determine if they sent more overseas than one-off victims. Figure 13 illustrates the distribution of total money sent overseas by both victims and those identified as possible repeat victims in the last two years. Some differences can be observed. For example, there were more repeat victims who sent more than $50,000 overseas. In addition, the largest number of one-time victims sent between $600 and less than $2,000, whereas for repeat victims the largest group sent between $3,000 and less than $6,000.

As the data were not normally distributed, the Mann-Whitney U test was used to see if the difference between the two groups in the amount sent overseas was statistically significant. For the total amount sent overseas in the previous two years, repeat victims sent significantly more money overseas than one-off victims ($z=-4.012$, $p<0.01$, $n=161$).

Figure 13: Distribution of the total amount of money sent overseas by victims and repeat victims in the two years prior to participating in the survey (n)

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

While there was a difference between the two groups when looking at the total amount sent overseas, when the largest amount sent in the previous two years was analysed, there was no significant difference in the amount sent by victims or repeat victims (see Table 29).

Table 29: Largest amount of money sent overseas during the last two years, victims and repeat victims

Amount sent	Victim		Repeat victim	
	n	%	n	%
$0–$199	1	1.0	0	3
$200–$299	3	2.9	3	5.2
$300–$399	3	2.9	0	0
$400–$499	2	1.9	2	3.4
$500–$599	3	2.9	4	6.9
$600–$999	16	15.5	2	3.4
$1,000–$1,999	16	15.5	10	17.2
$2,000–$2,999	7	6.8	6	10.3
$3,000–$5,999	15	14.6	8	13.8
$6,000–$9,999	10	9.7	4	6.9
$10,000–$14,999	9	8.7	2	3.4
$15,000–$29,999	8	7.8	7	12.1
$30,000–$49,999	5	4.9	4	6.9
$50,000–$200,000	4	3.9	4	6.9
$200,001 and over	1	1.0	1	1.7
Total	103		58	

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Principal reason for sending the largest amount of money

Respondents were asked about the largest funds transfer they had made in the two years prior to completing the survey. One of the questions asked respondents about the principal reason they decided to send money overseas for that transaction.

Table 30 illustrates the various reasons respondents sent money overseas that were not significantly associated with repeat victimisation.

Table 30: Principal reason for sending money overseas—victims and repeat victims			
Reason	df	χ^2	Significance
I wanted to make extra money	1	0.59	0.444
To obtain something I was entitled to receive	1	0.34	0.562
It was a unique opportunity	1	1.15	0.283
To help me with a personal or business problem	1	0.02	0.875
I was afraid not to respond[a]	n/a	n/a	n/a
A friend/family member told me that I should respond[a]	n/a	n/a	n/a
I wanted to help out the person seeking my assistance as a favour	1	2.58	0.108
I was told it was a loan and I would get my money back	1	3.57	0.059

a: Insufficient responses in categories to analyse the variable
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

As shown in Table 31, a significant relationship was found between repeat victimisation and transferring money overseas to buy goods and services online ($\chi^2(1,161)=9.92$, $p<0.01$, Cramér's V=-0.25). Repeat victims were significantly less likely than other victims to have transferred the largest amount of money for that reason (22% of repeat victims compared with 48% of victims).

Table 31: Contingency table for principal purpose for sending the largest amount of money overseas for purchasing goods and services and repeat victimisation					
	Principal reason: transferring money to purchase goods and services				Total
	Selected		Not selected		
	n	%	n	%	n
Repeat victim	13	22.4	45	77.6	58
Victim	49**	47.6	54	52.4	103
Total	62		99		161

**statistically significant at $p<0.01$
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Protective factors used by one-off and repeat victims

After examining the differences between the time spent by victims and non-victims using the internet and their ability to use IT, the same variables were re-examined using the victim and repeat victim groups. This was to see if experiences with IT and hours spent using the internet could help explain why some victims became repeat victims of online fraud.

Table 32: Repeat victims and level of knowledge about computers and other forms of IT					
Level of use	One-off victims		Repeat victims		Total
	n	%	n	%	n
Very low	0	0	1	1.7	1
Low	5	4.9	7	12.1	12
Moderate	51	49.5	22	21.4	73
High	32	31.1	20	34.5	52
Very high	13	12.6	5	8.6	18
No response	2	1.9	3	5.2	5
Total	103	100	58	100	161

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Table 32 shows how respondents self-reported their knowledge of using computers and other forms of IT. Some similarities existed between victims and repeat victims in their levels of knowledge about computers and other forms of IT. Chi-square tests were performed to see if there was an association between victimisation and the level of computer knowledge. The analysis showed there was not a significant relationship between repeat victimisation and levels of knowledge about computers ($\chi^2(4,161)=6.799$, $p=0.147$).

A significant association was found between level of IT knowledge and repeat victimisation when the variable 'level of knowledge about computers and other forms of IT' was separated into three categories of high to very high knowledge, moderate knowledge, and low to very low knowledge—nil responses were coded as low to very low knowledge—($\chi^2(2,161)=6.02$, $p<0.05$). Repeat victims were more likely (19% compared with 7%) than once-only victims of online fraud to self-report as having very low to low knowledge about computers and other forms of IT. No differences were found between victims and repeat victims and the ability to use computers and other forms of IT ($\chi^2(4,161)=7.77$, $p=0.100$; Table 33).

Table 33: Repeat victims and the ability to use computers and other forms of IT					
Level of use	One-off victims		Repeat victims		Total
	n	%	n	%	n
Very low	7	6.8	1	1.7	8
Low	0	0	3	5.2	3
Moderate	48	46.6	24	41.4	72
High	32	31.1	21	36.21	53
Very high	16	15.5	9	15.5	25
Total	103	100	58	100	161

Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Figure 14 illustrates the differences between victims and repeat victims in the number of hours spent on the internet. When the data were analysed to test the relationship, it was found the differences were not statistically significant ($\chi^2(5,161)=6.46$, $p=0.264$).

Figure 14: Hours spent on the internet by victims and repeat victims (%)

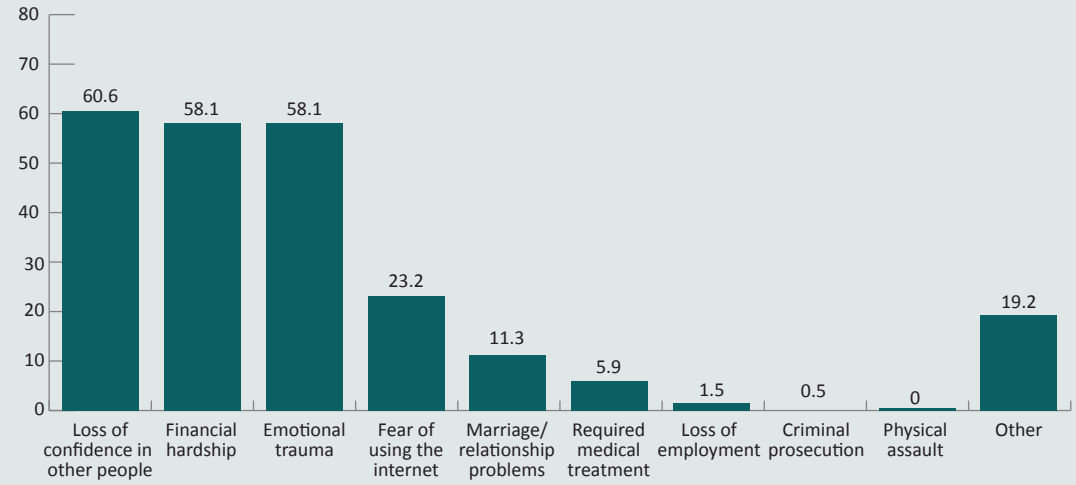
Note: Due to rounding, percentages may not total 100
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Consequences of victimisation

Victims of online fraud were asked about how their involvement in the fraud had affected them. Respondents were provided with a list of possible outcomes that might have occurred as a result of the victimisation, such as financial hardship, emotional trauma, relationship breakdowns, criminal prosecution, and fear of using the internet. Only respondents identified as victims from the survey data are discussed and analysed in this section.

As demonstrated by Figure 15, almost 61 percent of victims (n=123, 60.6%) indicated that they had lost confidence in other people as a result of their decision to send money overseas. Similarly, almost 60 percent of victims (n=118, 58.1%) indicated that they had experienced financial hardship and/or emotional trauma as a result of their involvement in such an undertaking. Almost one quarter of victims (n=47, 23.2%) indicated they feared using the internet following their victimisation.

Figure 15: Effects of involvement in online fraud for victims (%)



Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

The victim/repeat victim sample was analysed to see if there were any relationships between repeat victimisation and negative consequences as a result of engaging in the undertaking.

Table 34 illustrates the results of the chi-square tests for those outcomes that were found not to have a significant relationship with repeat victimisation and online fraud.

Table 34: Outcomes of online fraud that did not have a significant relationship with repeat victimisation in the past two years (n=151)

Outcome	df	χ^2	Significance
Emotional trauma	1	1.832	0.176
Marriage or relationship problems	1	0.245	0.621
Criminal prosecution[a]	n/a	n/a	n/a
Physical assault[b]	n/a	n/a	n/a
Loss of employment[b]	n/a	n/a	n/a
Fear of using the internet	1	2.703	0.100

a: No respondents indicated the outcome of online victimisation was criminal prosecution
b: Insufficient respondents indicated they had suffered physical assault or loss of employment as a result of online victimisation; therefore analysis could not be undertaken
Source: AIC Preventing Consumer Fraud Victimisation in Australia Survey 2015 [AIC dataset]

Repeat victims were more likely (76% compared with 45%) to experience financial hardship as a consequence of victimisation due to online fraud, than one-off victims ($\chi^2(1,161)=11.54$, $p<0.001$). The association between financial hardship and repeat victims of online fraud was a strong association with a Cramér's V of 0.32 (Table 35).

Table 35: Contingency table of the consequences of online fraud financial hardship and repeat or single-time victimisation

Victimisation type	Financial hardship				Total
	Selected		Not selected		
	n	%	n	%	n
Repeat victim	44***	75.9	14	24.1	58
Single-time victim	46	44.7	57	55.3	103
Total	90		71		161

***statistically significant at $p<0.001$
Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

In addition, repeat victims were more likely (12% compared with 3%) than one-off victims of online fraud to require medical treatment as a result of falling victim to the fraud. A Fisher's exact test was used given the small proportion of the sample indicating they required medical treatment. This test is a more conservative statistical measure and was used instead of a chi-square, as the assumption that there be no more than 20 percent of the expected frequencies with a value of less than five was violated ($p<0.05$, Fisher's exact; Table 36).

Table 36: Contingency table of the consequences of online victimisation and requiring medical treatment and repeat victims					
Victimisation type	Lack of confidence in others				Total
	Selected		Not selected		
	n	%	n	%	n
Repeat victim	7*	12.1	51	87.9	58
Single-time victim	3	2.9	100	97.1	103
Total	10		151		161

*statistically significant at $p<0.05$, Fisher's exact
Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

Negative life events

When examining the victim and non-victim sample there were very few significant associations between victimisation and negative life events. The same analyses were undertaken to see if there were associations between repeat victimisation and negative life events. Due to the low cell sizes in some of the expected frequencies, Fisher's exact tests were performed. Table 37 presents the negative life events that did not have a significant relationship with repeat victimisation.

Table 37: Fisher's exact tests for life events		
Life event	df	*p*-value
Have you ever been declared bankrupt	3	0.319
In last five years death of a family member or friend	3	0.778
In last five years suffered depression	3	0.235
In last five years lost job	3	0.472
In last five years diagnosed with serious illness	3	0.432
In last five years victim of serious accident	2	0.692
In last five years were the victim of any other kind of serious crime	2	0.725

Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

One negative life event was found to have a significant association with repeat victimisation—those respondents who suffered a marriage or relationship breakdown in the past five years. As seen in Table 38, repeat victims were more likely to have had a relationship breakdown in the last five years prior to victimisation, than one-time victims (Fisher's exact, $p<0.05$).

Table 38: Contingency table for life event, in previous five years suffered a marriage or relationship breakdown and repeat or single-time victimisation via online fraud

Victimisation	Relationship breakdown in past five years n (%)			Total
	Selected	Not selected	I'd rather not say	
Repeat victim	16*(27.6)	40 (69.0)	2 (3.5)	58
One-off victim	16 (15.5)	87 (84.5)	0	97
Total	32	127	2	161

*statistically significant at $p<0.05$, Fisher's exact
Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

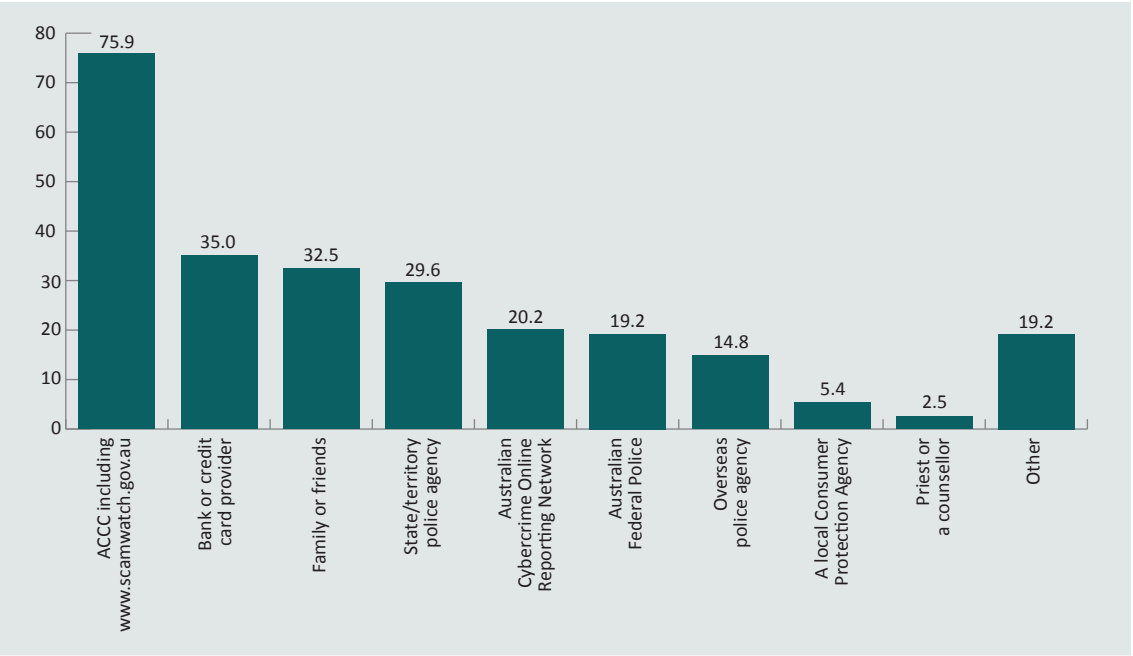
Reporting to authorities

Respondents were asked if they reported their involvement in the activity to anyone, and if so, who they informed. They could select more than one option from the list provided in the survey questionnaire.

As shown in Figure 16, most victims (75.9%) informed the ACCC either directly, or via the Scamwatch website. This was not surprising, given the victim sample was drawn from an ACCC database of individuals who had made a report to the Scamwatch website.

Apart from the ACCC, victims also identified bank or credit card providers (35%), family or friends (32.5%), and state/territory police agencies (29.6%) as common entities that they informed about their involvement in potentially fraudulent undertakings. Victims were least likely to inform a priest or a counsellor about their involvement in a potential fraud, with only 2.5 percent of victims indicating they would inform such people (see Figure 16).

Figure 16: Entities that victims informed about their decision to send money overseas



Source: Preventing Consumer Fraud in Australia survey 2015 [AIC dataset]

If respondents advised they had not reported their victimisation to anyone, they were asked about their reasons for not reporting their experiences. The most common reason was embarrassment (8.9%, n=18), followed by the belief that police would be unable to find the offender in any event (5.9%, n=12), and uncertainty on the part of the victim as to whom they should report (5.9%, n=12).

No statistically significant differences were found between victims and repeat victims, and reporting or not reporting their victimisation.

Discussion

At the end of December 2017 there were 14.2m internet subscribers in Australia, an increase of 3.4 percent from the end of June 2017 (ABS 2018). The way that people use the internet for recreation or for buying goods and services raises a number of important questions relevant to their risk of being victimised, including why some people experienced more problems than others as a result of their online interactions.

Online fraud has become one of the most prevalent international crimes (UK Audit Office 2017; Williams 2016). In the year ending 30 June 2016, out of 11.8 million reported crimes in the UK, 3.6 million were fraud-related, and of those 3.6 million, 1.9 million were cyber-related frauds (UK Audit Office 2017). In Australia the ABS estimated for 2014–15 that 1.6 million Australians (8.5% of the population 15 years and over) experienced personal fraud, with losses for all personal fraud (including scams, credit card fraud and identity crime) reaching $3b (ABS 2016). In 2017, the ACCC, ACORN and other government organisations such as the Australian Taxation Office received more than 200,000 scam reports with total losses exceeding $340m—an increase of $40m over 2016 losses. The ACCC alone received more than 161,500 scam reports with $90.9m in financial losses, which represents an eight percent increase in reported losses over 2016 (ACCC 2018). Online fraud in Australia is a costly and potentially devastating crime.

This study sought to determine and to quantify the factors that make an individual vulnerable to online fraud and lead to victimisation. Using a methodology similar to that used with case-control samples in epidemiological studies, two independent samples were examined—one of victims and another of non-victims, all of whom had sent money overseas in the past two years. A number of factors were examined to determine how the two groups differed and why some people became victims while others did not. Factors examined included: online behaviour, demographic factors, and the effects of important life events. A small number of statistically significant findings were identified which may be useful in guiding the development of targeted awareness-raising and online fraud prevention programs in the future. Interestingly, many of the findings did not demonstrate statistically significant relationships between variables that were expected to have been indicative of vulnerability to consumer fraud.

Factors that make a victim of online fraud

Respondents were exactly matched on age, gender and education, so no statistical analysis involved those variables. The highest percentage of victims (29.5%) were aged 65 years and over. This would appear to be consistent with research by Jorna (2016b) who found that respondents aged 65 years and over were more likely than other age groups to send money in response to a fraudulent invitation.

The present research also showed that respondents who were found to be victims of online fraud had not attained levels of education as high as those who were non-victims. An individual's level of education has been found to impact consumer fraud vulnerability in a number of ways. For example Titus and Gover (2001) found that more highly-educated individuals were more likely to fall victim to personal fraud. Conversely, Lee and Soberon-Ferrer (1997) found that an individual's level of education influenced consumer vulnerability to fraud, with less-educated individuals found to be more vulnerable to consumer fraud than more highly educated individuals.

The current study also found a high percentage of victims who did not conduct any research into the entity requesting money prior to making an overseas payment. Just over 47 percent of victims (47.3%) and 67 percent of non-victims indicated that they did not conduct any research prior to sending money overseas. For non-victims, this high percentage could be explained by the fact that a number of them were sending money overseas for family reasons or making purchases on well-known websites such as eBay and Amazon.

Little research is available that looks at the effectiveness of different ways of researching an online opportunity. Nor is information provided on how to use review sites or how to research different overseas businesses and organisations. While victims reported conducting research on online opportunities more frequently, when the type of research undertaken was explained it was not an adequate preventive measure. Button et al. (2014) found it was difficult for victims to detect if a website was false or legitimate as the scammers have begun using professionally designed websites and references to well-known and legitimate companies. The research conducted by Button et al. (2014) found victims had contacted the websites used by scammers and rung the scammers, unaware they were providing false information. This is similar to the findings in the present research where victims were found to have used websites provided by scammers, while non-victims would use other searches to review the websites or opportunities.

Conversely, the high percentage of victims who sent money overseas without conducting any research is concerning. This finding may support the idea that victims are more likely to be impulsive and have lower levels of self-control compared with non-victims (Holtfreter et al. 2010). Indeed, the desire to act quickly and without thinking through the possible risks involved in acting upon a fraudulent online invitation or offer may explain why such a high percentage of victims failed to research the entity requesting their money before they decided to make the payment. This finding also indicates a need for future awareness-raising and prevention programs to emphasise the need for individuals to research entities requesting money prior to engaging with them and actually carrying out the payment request.

When asked about the funds transfer method used to make the overseas payment, the most common method used by victims was money wire transfer (43.3%), followed by electronic funds transfer using a bank (37.4%), and credit card transactions (9.9%). By contrast, only 10.3 percent of non-victims indicated that they used money wire transfers to transfer funds overseas, with the most common funds transfer method for non-victims being escrow services such as PayPal (40.2%). This was followed by electronic funds transfer using a bank (19.9%) and credit card transactions (18.7%).

While a number of consumer protection campaigns and programs have sought to educate individuals about the risks involved in using money wire transfers to make overseas payments (eg Western Union Fraud Awareness Campaigns, as well as the fraud awareness materials published by the ACCC and Scamwatch), it would appear that there is a continuing need for individuals to be reminded of these risks. In particular, the regression model demonstrated the importance of financial institutions and money transfer businesses when it comes to reducing victimisation by scammers. Victims were more likely than non-victims to use methods such as money wire transfers and other forms of electronic funds transfers, a fast way for sending money that can then be instantly transferred elsewhere. It may be prudent for future online fraud awareness-raising and prevention programs to reiterate the risks of online fraud victimisation when individuals are requested to make payments via money wire transfer. Bank staff who become aware of large suspicious transactions from at-risk demographics can often alert their customers to the presence of fraud risks and prevent further victimisation. In one recent case in Western Australia, a 65-year-old woman was persuaded by a man she met on a dating website to send $468,000 to him, until her bank alerted her to the likelihood of her involvement in a consumer fraud (see Hamlyn & Moussalli 2019).

One of the limitations of self-report surveys such as the one used in this study is the fact that people do not always accurately report their victimisation experiences (Lee & Soberon-Ferrer 1997). In the current study, embarrassment was the most common reason cited by victims for not reporting their involvement in the fraud (8.9%, n=18), followed by the belief that police would be unable to find the offender in any event (5.9%, n=12) and uncertainty on the part of the victim as to whom they should report (5.9%, n=12). These results are consistent with other studies that have examined the reasons behind victims' reluctance to report online fraud. They have also found feelings of shame and embarrassment (Cross 2015; Ross & Smith 2011), and the belief that the police would be unable to find the offender (Ross and Smith 2011) to be some of the more common reasons provided by victims for their decision not to report their victimisation.

Protective factors

The present research found victims spent significantly less time using the internet than non-victims, with non-victims more likely to spend 10 hours or more using the internet than victims. The differences in time spent on the internet by victims and non-victims each week may be attributed to concern by victims that they may become victims of online fraud again. Indeed, Reisig, Pratt and Holtfreter (2009) found that individuals who perceived themselves to be at greater risk of online theft victimisation modified their online behaviours to reduce the likelihood that they would be victimised. This included spending less time on the internet. However, with everyday activities becoming increasingly based online, spending less time on the internet is not an achievable method of preventing online fraud. Rather it may mean consumers do not have enough experience online to effectively use protective measures when they do go online. Bossler and Holt (2009) examined the time spent online through a Routine Activity Theory perspective, noting that experience online had the potential to be an effective capable guardian while online. That research found that people engaging in everyday online activities, such as internet banking or online shopping, were not associated with online fraud victimisation. However, people who engaged in online piracy did increase their risk of victimisation (Bossler & Holt 2009).

The use of computer and IT security presented mixed results in the present research. Initial findings indicated the use of more advanced forms of IT security may represent a preventative factor against online fraud victimisation. Non-victim respondents were more likely to use security measures such as anti-phishing software, anti-spyware, and content and imaging filtering while online compared with respondents identified as victims. This indicates that a greater level of use and understanding about computer security may help to prevent online fraud. However, when a 'computer security' variable was recoded to factor in the types of advanced security measures used by respondents, there was no significant difference between victims and non-victims using a few or more forms of security. Whitty (2017), in a study looking at the psychological characteristics of romance scam victims, asked respondents (victims and non-victims) to self-rate their level of understanding about cybersecurity, on the basis that those who reported they did not know a lot about cybersecurity were more likely to be victims of romance scams. Consistent with the current research, Whitty (2017) found the hypothesis about knowledge of cybersecurity was not statistically proven. Bossler and Holt (2009) found no link between computer security and online victimisation. In fact they found 25 percent of computer systems that were protected with some form of security contained malware, where 33 percent of non-protected computer systems contained malware.

The other component of protective factors related to personality traits. The present research did not use scale questions to determine different personality types of victims such as low self-control (Gottfredson & Hirschi 1990; Holtfreter et al. 2010); or kindness, greed or impulsivity and the like (Whitty 2017). Rather, respondents were asked to assess how likely or unlikely they were to do certain things, such as trust strangers, help those in need or make impulsive decisions. One problem with this method was that respondents were only asked these questions once, so it could not be seen if there had been a change in how victims perceived themselves based on their being a victim of online fraud, or if that was how they perceived themselves all the time.

The logistic regression model examining victimisation, computer security, hours spent using the internet and propensity to trust strangers or help those in need found non-victims were more likely to trust strangers and help those in need. Victims were either unlikely or very unlikely to describe themselves as willing to help those in need, and also described themselves as unlikely to trust strangers. This is somewhat counter-intuitive given victims were more likely to send money to people they had only met online or strangers. This is an area that requires more study. Some research has looked at psychological factors that may contribute to online fraud victimisation; however, very little has examined Australian victims and whether or not there are differences between overseas and Australian victims (Modic & Lea 2012; Whitty 2017).

Victimisation

The present study found that differences between repeat victims and one-time victims were almost the same as those found between victims and non-victims, with repeat victims more likely to send money to people they did not know or whom they had only met online. A considerable amount of research has been done around the needs of mass-marketing and advance fee fraud victims (Buchanan & Whitty 2014; Button et al. 2014; Whitty 2017). However, while many of those victims are repeat victims, the research does not specifically examine if the needs of repeat victims of online fraud differ from one-off victims, and how organisations can support those victims. Cross (2013) found it was common for victims of online fraud to conduct multiple money transfers over a period of time, often only stopping when they had run out of money or had realised that the opportunity was fraudulent.

No widely agreed definition of repeat victim of online fraud exists. The present study defined a repeat victim as one who had sent amounts of money overseas on multiple occasions. Other studies have defined a repeat victim as someone who has been victimised by multiple online frauds—whether emanating from the same or various offenders. The lack of research on repeat victims of online fraud, and clarity about what constitutes a repeat victim, requires further consideration. As online crime becomes more prolific, there is a greater need to understand what makes someone vulnerable to repeat online fraud victimisation.

Victims of online fraud can experience serious consequences (Cross, Smith & Richards 2014) and the present research found that repeat victims of online fraud might suffer more than others. Repeat victims are more likely than one-time victims to face financial hardship as a consequence of online fraud. They are also more likely than one-time victims to require medical attention as a consequence of online fraud victimisation. This means repeat victims have a unique set of support needs, including the need for counselling, and education on financial literacy.

Theoretical implications

Three potential explanations for victimisation through online fraud based on criminological theory were outlined above: Self-Control Theory (Gottfredson & Hirschi 1990); Routine Activity Theory (Cohen & Felson 1979); and Lifestyle-Exposure Theory (Hindelang, Gottfredson & Garofalo 1978). In addition, the impact that negative life events can have on an individual's cognitive judgment and their ability to process information and make sound decisions (Lee & Soberon-Ferrer 1997) was also offered as a potential explanation for victimisation of individuals with certain backgrounds.

The present study tested a number of aspects of these theoretical positions, with varying outcomes. The findings were contradictory in terms of impulsivity, with victims reporting being very unlikely to make impulsive decisions, but also very unlikely to wait for something due to them. These characteristics were not, however, statistically predictive of victimisation in the regression model presented.

In terms of Routine Activity Theory, victims used the internet for less time, on average, than non-victims but used computer security measures more frequently than non-victims. This latter finding showed a statistically weak level of association that was not predictive of victimisation in the regression model presented. However, the hypothesis that greater familiarity with online activities would result in a reduced likelihood of victimisation was supported. Victims of online fraud were also more likely to use payment mechanisms that would not provide compensation in cases of fraud, such as electronic funds transfers, as opposed to credit card or PayPal. Arguably the use of payment systems that allow for reimbursement in the case of fraud shows some enhanced influence of capable guardianship.

In relation to Lifetime Exposure Theory, evidence that negative life events are predictors of victimisation was not found in the regression model outcomes. The only life event that was found to have a significant association with victimisation was relationship breakdown, but when this was included in the model, it was not a statistically significant predictor of victimisation. None of the demographic or behavioural factors or negative life events was predictive of victimisation.

Policy implications

The present study identified several opportunities that policymakers, police, consumer affairs organisations and financial institutions may want to take advantage of to improve the targeting of online consumer fraud prevention and awareness-raising initiatives in the future. The first of these relates to the 47 percent of victims who sent money overseas without conducting any research about the entity requesting the payment—the fact that victims were found to send larger amounts of money overseas compared with non-victims, and that victims sent money using payment mechanisms that did not offer reimbursement in the case of fraud.

The desire to act quickly and without thinking through the possible risks involved in acting upon a fraudulent online invitation or offer may explain why such a high percentage of victims failed to research the entity requesting their money before they decided to make the payment. This finding suggests that future awareness-raising and prevention programs should emphasise the need for individuals to research those requesting money before engaging with them and completing the payment request. Consideration could also be given to exploring more invasive preventive and disruptive actions such as allowing financial institutions and remitters to refuse to transfer funds where definitive evidence is present that the account holder is currently being defrauded.

The fact that the current study identified victims as being more likely to send money overseas via money wire transfer compared with non-victims also highlights the continuing need for consumer protection campaigns and programs to educate and remind individuals of the risks of using money wire transfers when making overseas payments. Awareness campaigns of this nature are currently being undertaken by some of the largest corporate remitters.

A statistically significant relationship was found between victimisation and the amount of money that was sent overseas, with victims sending more money overseas during the last two years compared with non-victims. This finding reinforces the need to have programs such as the ACCC's Scams Disruption Project (ACCC 2018), South Australia Police's Operation Disrepair (Nankervis 2014) and Project Sunbird (WA Department of Commerce 2014)—all recently withdrawn due to limited resources. Given the large amounts of money lost to online fraud in Australia every year, it may be prudent for such proactive initiatives to be reintroduced in each of the Australian states and territories. The financial intelligence collected by the Australian Transaction Reports and Analysis Centre (AUSTRAC) will be important, but the information may need to be shared with a larger pool of entities, including those in the private sector, than is currently permitted.

Those victims who are sending multiple amounts of money overseas in response to the same or different fraud opportunities need to be identified. Repeat victims suffer more severe consequences as a result of online fraud than other victims. They face financial hardship given the large sums of money transferred, and they may require medical assistance, for example counselling. Little research exists about the specific needs and vulnerabilities faced by repeat victims of online fraud. However, the preliminary research explored here has highlighted several areas of concern for these types of victims.

Online fraud is fast becoming one of the most prevalent and costly crimes of the 21st century. With more services going online, the factors contributing to some people becoming victims of online fraud need to be determined as well as what can be done to reduce risks of victimisation. This research has explored various factors that might contribute to why some people experience victimisation online and why others do not, such as the reason people transfer money overseas, how the transfer process occurs, and the amount of money transferred. While education about online fraud has been a priority of Australian governments, more needs to be done to keep people safe while online.

A large proportion of victims in the present study reported that they researched the opportunities presented to them. However, when examined in detail the research undertaken was superficial and ineffective in determining risk. Perhaps more information needs to be provided on how to research a company or individual online or what are some legitimate review websites for online products and services. Reducing the risk of online fraud is not the responsibility of Australian governments alone. It requires a collaborative effort between governmental, non-profit and other businesses to educate consumers about how to interact safely with others online. Education about fraud must also target certain areas, such as identifying false websites, how to identify legitimate websites and, for banks and money transfer companies to be aware when someone may be victim of a fraud. These strategies will help consumers to increase their own awareness of fraud risks and reduce their vulnerabilities.

This study provides new data to support the development of targeted online fraud awareness-raising campaigns. These could focus on areas of online behaviour most likely to lead to victimisation. Further research could be conducted to verify whether the factors that were found to be statistically significant predictors of victimisation in the present study remain so when their presence before and after victimisation is taken into account.

References

URLs current as at February 2019

Anderson K 2013. *Consumer fraud in the United States, 2011: The third FTC survey.* https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey

Australian Bureau of Statistics 2018. *Internet Activity, Australia,* December 2017. ABS cat. no. 8153.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0

ABS 2017. *Internet Activity, Australia,* December 2016. ABS cat. no. 8153.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0

ABS 2016. *Personal Fraud,* 2014–15. ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0

ABS 2012. *Personal Fraud,* 2010–11. ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/4528.0

Australian Competition and Consumer Commission (ACCC) 2018. *Targeting scams: Report of the ACCC on scams activity in 2017.* Canberra: ACCC

ACCC 2015. *Targeting scams: Report of the ACCC on scams activity in 2014.* Canberra: ACCC

Atkins B & Huang W 2013. A study of social engineering in online frauds. *Open Journal of Social Sciences* 1(3): 23–32

Bernard T, Snipes J & Gerould A 2010. *Vold's theoretical criminology.* New York: Oxford University Press

Bossler AM & Holt TJ 2009. On-line activities, guardianship and malware infection: An examination of Routine Activities Theory. *International Journal of Cyber Criminology* 3(1): 400–420

Buchanan T & Whitty M 2014. The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law* 20(3): 261–283

Button M, McNaughton Nicholls C, Kerr J & Owen R 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408

Button M, Lewis C & Tapley J 2009. *Fraud typologies and victims of fraud: Literature review.* London: Office of Fair Trading and National Fraud Authority

Chang J 2008. An analysis of advance fee fraud on the internet. *Journal of Financial Crime* 15(1): 71–81

Chang J & Chong M 2010. Psychological influences in e-mail fraud. *Journal of Financial Crime* 17(3): 337–350

Cohen & Felson 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588–608

Corby G 2009. *A dead man fell from the sky – Ancient Greek insurance scams.* http://www.garycorby.com/2009/02/ancient-greek-insurance-scams.html

Cross C 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21(2): 187–204

Cross C 2013. 'Nobody's holding a gun to your head…' Examining current discourses surrounding victims of online fraud, in Richards K & Tauri J (eds), *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference,* Crime and Justice Research Centre, Queensland University of Technology: 25–32

Cross C & Blackshaw D 2014. Improving the police response to online fraud. *Policing:* 1–10

Cross C, Smith RG & Richards K 2014. Challenges of responding to online fraud victimisation in Australia. *Trends & issues in crime and criminal justice* no. 474. https://aic.gov.au/publications/tandi/tandi474

Dhamija R, Tygar J D & Hearst M 2006. *Why phishing works: Experimental social science laboratory (Xlab).* UC Berkeley: Experimental Social Science Laboratory (Xlab). http://escholarship.org/uc/item/9dd9v9vd#page-1

Gottfredson M R & Hirschi T 1990. *A general theory of crime.* California: Stanford University Press

Hamlyn C & Moussalli I 2019. *Online scams surge in 2019 with WA victims ripped off by more than $1.8 million.* ABC News, 7 February. https://www.abc.net.au/news/2019-02-07/online-scams-surge-in-bad-start-to-2019/10789528

Holt T & Bossler A 2008. Examining the applicability of Lifestyle-Routine Activities Theory for cybercrime victimization. *Deviant Behavior* 30(1): 1–25

Hindelang M, Gottfredson M & Garofalo J 1978. *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Ballinger Publishing Company: Massachusetts

Holtfreter K, Reisig M, Leeper Piquero N & Piquero A 2010. Low self-control and fraud—Offending, victimization, and their overlap. *Criminal Justice and Behavior* 37(2): 188–203

Holtfreter K, Reisig M & Pratt T 2008. Low self-control, routine activities, and fraud victimization. *Criminology* 46: 189–220

Hutchings A & Hayes H 2009. Routine Activity Theory and phishing victimisation: Who gets caught in the 'Net'? *Current Issues in Criminal Justice* 20(3): 1–20

Jorna P 2016a. *Australasian Consumer Fraud Taskforce: Results of the 2014 online consumer fraud survey.* Research Report no. 1. Canberra: AIC. https://aic.gov.au/publications/rr/rr001

Jorna 2016b. The relationship between age and consumer fraud victimisation. *Trends & issues in crime and criminal justice* no. 519. Canberra: AIC. https://aic.gov.au/publications/tandi/tandi519

Lee J & Soberon-Ferrer H 1997. Consumer vulnerability to fraud: Influencing factors. *Journal of Consumer Affairs* 31(1): 70–89

Modic D & Lea SE (2012). *How neurotic are scam victims, really? The big five and Internet scams.* http://ssrn.com/abstract=2448130

Nankervis 2014. Operation Disrepair finds South Australians lost more than $2 million in 4261 transactions to foreign scams. *The Advertiser.* http://www.adelaidenow.com.au/news/south-australia/operation-disrepair-finds-south-australians-lost-more-than-2-million-in-4261-transactions-to-foreign-scams/story-fni6uo1m-1226842491763

Nhan J, Kinkade P & Burns R 2009. Finding a pot of gold at the end of an internet rainbow: Further examination of fraudulent email solicitation. *International Journal of Cyber Criminology* 3(1): 452–475

Pearce N 2016. Analysis of matched case-control studies. BMJ: 2016 352:i969 http://www.bmj.com/content/352/bmj.i969

Pratt T, Holtfreter K & Reisig M 2010. Routine online activity and internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency* 47(3): 267–296

Reisig MD, Pratt TC & Holtfreter K 2009. Perceived risk of internet theft victimisation: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior* 36: 369–384

Ross S & Smith RG 2011. Risk factors for advance fee fraud victimisation. *Trends & issues in crime and criminal justice* no. 420. Canberra: AIC. https://aic.gov.au/publications/tandi/tandi420

Shadel D, Pak K & Sauer J 2014. *Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim.* Washington, DC: AARP Research. https://doi.org/10.26419/res.00076.004

Tabachnick BG, Fidell LS & Osterlind SJ 2001. *Using multivariate statistics,* 4th ed. Needham Heights, MA: Allyn & Bacon

Titus RM & Gover AR 2001. Personal fraud: The victims and the scams. *Crime Prevention Studies* 12: 133–151

United Kingdom National Audit Office 2017. *Online fraud.* HC 45. London: National Audit Office. https://www.nao.org.uk/report/online-fraud/

United Kingdom Office of Fair Trading (OFT) 2006. *Research on impact of mass marketed scams.* OFT883. London: OFT

van Wilsem J 2013. 'Bought it, but never got it' Assessing risk factors for online consumer fraud victimization. *European Sociological Review* 29(2): 168–178

Van Wyk J & Benson M 1997. Fraud victimization: Risky business or just bad luck? *American Journal of Criminal Justice* 21(2): 163–179

Western Australia Department of Commerce 2014. WA Scamnet website: *Project Sunbird flying high.* http://www.scamnet.wa.gov.au/scamnet/Scam_Types-Advanced_fee_frauds-OperationProject_Sunbird.htm

Whitty M 2017. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior and Social Networking* 21(2): 105–109

Williams ML 2016. Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology,* 56: 21–48

Yar M 2005. The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology* 2(4): 407–427

Appendix A: Preventing consumer fraud victimisation in Australia survey

This survey examines your experiences as a consumer when using online services over the last two years. The way people use the Internet for recreation or for buying goods and services raises many important questions including why some people experience more problems than others. Your answers will provide information that can be used to improve consumer protection for all Australians who participate in the online world of today.

You will be asked to answer some questions about your:

- Consumer activities including payments made overseas in response to requests from people online;
- Any consequences you have experienced as a result;
- Whether you reported what happened, and to whom;
- Some background information about your age, gender, residence, income, language at home, Indigenous background, education and computer usage (this will help us find out which people are experiencing problems online);
- Your recent life experiences including major life events that you have experienced (again, this will help us to find out if particular people become victims of scams more than others).

The survey will take approximately 10 minutes of your time. Your answers will be completely anonymous and the results will not be able to identify you personally in any way. Your participation is entirely voluntary, and your responses will not be able to be used for official investigations.

If you feel uncomfortable about answering any questions you can choose not to reply to some or all of the questions, and you may withdraw at any stage. If you decide to withdraw, any information that you have already provided will not be used in the research study. However, we hope that you will try to complete the survey in full.

If you would like to speak to someone after the research has been completed to obtain advice or support, Lifeline provides crisis support by telephone 24 hours a day on 13 11 14 (at the cost of a local call), or online at https://www.lifeline.org.au/Get-Help/Online-Services/crisis-chat between 8pm and midnight. You should also contact your local police if you suspect that you have been a victim of online fraud.

The results of the survey will be available from the Australian Institute of Criminology's website early in 2016, at www.aic.gov.au. You can obtain further information from [email] who is in charge of the study. If you have any ethical concerns or complaints about the study, please contact [email] or [phone number].

Thank you for participating in this research, your involvement is greatly appreciated.

Please now answer the following questions.

Background information

Question 1. Please indicate the postcode and place of your usual place of residence?

Postcode in Australia—Please specify ☐

State or territory—Please specify ☐

☐ I do not normally reside in Australia

Question 2. What is your gender?

(Select one only)

☐ Male

☐ Female

☐ Other

Question 3. Which age group do you belong to?

(Select one only)

☐ 14 years and under

☐ 15–17 years

☐ 18–24 years

☐ 25–34 years

☐ 35–44 years

☐ 45–54 years

☐ 55–64 years

☐ 65 years and over

Question 4. What language is most often spoken at your home?

Please specify one language ☐

Question 5. Do you identify as Aboriginal or Torres Strait Islander?

(Select one only)

☐ Yes - Aboriginal

☐ Yes - Torres Strait Islander

☐ Yes - both Aboriginal and Torres Strait Islander

☐ No

☐ I'd rather not say

Question 6. What is the highest educational level you have completed?

(Choose one only)

☐ Primary schooling only

☐ Secondary schooling

☐ Tertiary (Undergraduate or Bachelor's Degree - pass or honours)

☐ Tertiary (Postgraduate Degree - masters or doctorate)

☐ Professional qualification without a degree

☐ Other—Please specify ☐

Question 7. How do you rate your level of knowledge and ability to use computers or other forms of IT?

(Please rate according to the following scale):

	Very low	Low	Moderate	High	Very high
Level of knowledge	☐	☐	☐	☐	☐
Ability to use	☐	☐	☐	☐	☐

Question 8. What was your individual gross income from all sources for the last financial year (ie. before tax has been deducted)?

☐ $0 - $18,200

☐ $18,201 - $37,000

☐ $37,001 - $80,000

☐ $80,001 - $180,000

☐ $180,001 and over

☐ I'd rather not say

Question 9. How many hours each week do you spend using the Internet including for email (include both time on work and personal use)?

(Choose one only)

- ☐ Never use the Internet
- ☐ 1 or less
- ☐ 2 - 4
- ☐ 5 - 9
- ☐ 10 - 19
- ☐ 20 or more

Question 10. Which of the following computer security measures do you use?

(Choose all that apply)

- ☐ Using passwords to logon
- ☐ Physically securing computers or wireless devices
- ☐ Encryption of data
- ☐ Anti-spam filters
- ☐ Anti-virus software
- ☐ Anti-spyware software
- ☐ Anti-phishing software
- ☐ Internet content / image filtering or monitoring
- ☐ Firewall
- ☐ Other—Please specify _____
- ☐ None
- ☐ Don't know

Online consumer activities

These questions ask about your online consumer activities

Question 11. During the last two years, have you sent money overseas?

- ☐ Yes
- ☐ No

Question 12. If you answered YES to Question 11, for what purpose did you send the money overseas?

(Choose all that apply)

- ☐ Paying for goods and services purchased other than on the Internet
- ☐ Paying for goods and services purchased online
- ☐ Business transactions
- ☐ Subscriptions to organisations overseas
- ☐ Sending money to friends I've met online
- ☐ Sending money to relatives or friends, other than those I've met online
- ☐ Sending money to people not personally known to you
- ☐ Donations to charities
- ☐ Fees, taxes or charges
- ☐ Other—Please specify

Question 13. Were you completely satisfied with the goods, services or benefit that you expected to receive in return for the overseas payment(s) you made?

- ☐ Yes
- ☐ No—Please describe why you were not completely satisfied

The following questions ask about the occasion when you sent the largest sum of money overseas during the last two years

Question 14. Which country did you send the largest sum of money to over the last two years?

(Please specify one country only)

Question 15. When you sent the largest sum of money overseas in the last two years, was this in response to a contact from someone you didn't know?

- ☐ Yes
- ☐ No (If you already knew this person, how did you know them? eg. I met them online)

Please specify

Question 16. When contact was first established with the person or organisation to whom you sent the largest sum of money overseas in the last two years, how did this occur?

- ☐ Mail
- ☐ Email
- ☐ SMS
- ☐ Phone
- ☐ Introduced or referred by someone else
- ☐ Face-to-face meeting
- ☐ On an online dating site
- ☐ Internet site
- ☐ Social media site

Please specify which social media site was used

- ☐ Other—Please specify

Question 17. When you were asked to send money overseas, what was the basis of this request?

(Choose all that apply)

- ☐ A payment in connection with an online purchase or sale of goods or services
- ☐ An offer of a job or acting as an employee or consultant
- ☐ The opportunity to gain a financial reward
- ☐ Assisting another person or agency with the distribution of charitable funds
- ☐ Participation in a lottery or other prize competition
- ☐ Helping someone to recover money that was owed to them
- ☐ Assisting a foreign dignitary
- ☐ Refund of bank fees, taxes or government benefits or an over-invoiced contract
- ☐ Unclaimed bank account
- ☐ Providing money to help someone I'd met online
- ☐ Cleaning "black cash"
- ☐ Transfer of funds from deceased estate
- ☐ Other—Please specify

Question 18. Did you send money to any person or organisation as a result of any of these requests?

☐ Yes

☐ No

☐ I'd rather not say

Question 19. Before you sent this money overseas, did you discuss the matter with friends or family?

☐ Yes

☐ No

Question 20. Before you sent this money overseas, did you undertake any research on the Internet or elsewhere about the person or organisation with whom you were dealing or the proposal involved?

☐ Yes (If yes, what kind of information or documents did you find or receive?)

Please specify

☐ No

Question 21. Did you do anything else to verify the identity of the person or organisation that you were dealing with?

☐ Yes (If yes, what did you do?)

Please specify

☐ No

Question 22. How much money did you send overseas for the largest transaction during the last two years?

☐ Nothing

☐ Don't know / can't remember

☐ I'd rather not say

☐ The following amount (If you aren't sure, please estimate the amount)

$

Question 23. How much money have you sent overseas all together during the last two years in relation to this undertaking?

- ☐ Nothing
- ☐ Don't know / can't remember
- ☐ I'd rather not say
- ☐ The following amount (If you aren't sure, please estimate the amount)

$ ☐

Question 24. Has a bank or other organisation recovered money that you have sent overseas in response to this undertaking?

- ☐ Yes
- ☐ No
- ☐ Not applicable

Question 25. If you answered YES to Question 24, how much money was recovered?

- ☐ Nothing
- ☐ Don't know / can't remember
- ☐ I'd rather not say
- ☐ The following amount? (If you're not sure, please estimate the amount)

$ ☐

Question 26. For the largest funds transfer overseas in the last two years, which funds transfer method did you use? (Choose one only)

- ☐ Cash in mail
- ☐ Cheques in mail
- ☐ Credit card transactions
- ☐ Pre-paid debit card transactions (eg Australia Post "Load & Go")
- ☐ Electronic Funds Transfer using a bank (direct credit)
- ☐ Escrow services (eg PayPal)
- ☐ Money wire transfers (eg Western Union, TravelEx etc.)
- ☐ Alternative remittance agents (eg hawala)
- ☐ Digital currencies (eg Bitcoin)
- ☐ Other—Please specify ☐

Question 27. For the largest funds transfer sent overseas in the last two years, what was the principal reason that you decided to send money? (Choose all that apply)

- ☐ I wanted to make extra money
- ☐ I wanted to buy goods and services
- ☐ To obtain something that I was entitled to receive
- ☐ It was a unique opportunity
- ☐ To help me with a personal or business problem
- ☐ I was afraid not to respond
- ☐ A friend / family member told me that I should respond
- ☐ I wanted to help out the person seeking my assistance as a favour
- ☐ I was told it was a loan and I would get my money back
- ☐ Other—Please specify

Question 28. In what ways has your involvement in this undertaking affected you? (Choose all that apply)

- ☐ Financial hardship
- ☐ Emotional trauma
- ☐ Marriage/relationship problems
- ☐ Criminal prosecution
- ☐ Physical assault
- ☐ Loss of employment
- ☐ Loss of confidence in other people
- ☐ Required medical treatment
- ☐ Fear of using the internet
- ☐ Other—Please specify

Question 29. Have you reported your involvement in this undertaking to anyone?

- ☐ Yes
- ☐ No

Question 30. If you answered YES to Question 29, who did you inform about your involvement?

(Choose all that apply)

- ☐ Australian Competition and Consumer Commission (ACCC) including www.scamwatch.gov.au
- ☐ Australian Cybercrime Online Reporting Network (ACORN) www.acorn.gov.au
- ☐ A local Consumer Protection Agency
- ☐ Family or friends
- ☐ Priest or a counsellor
- ☐ State/territory police agency
- ☐ Australian Federal Police
- ☐ Overseas police agency
- ☐ Bank or credit card provider
- ☐ Other—Please specify

Question 31. If you did not report to anyone, what were the reasons for not reporting? (Choose all that apply)

- ☐ I was embarrassed or felt foolish
- ☐ The police would be unable to find the offender
- ☐ Not much money was lost
- ☐ Insufficient evidence to give to the police
- ☐ I am in fear for my personal safety if I report it
- ☐ I am afraid that I may be prosecuted for my involvement
- ☐ Didn't know who to report to
- ☐ I still believe that I may recover my money
- ☐ Other—Please specify

About you

The next section of this survey asks about yourself and things that might have happened to you.

Question 32. Please describe how likely you are to do each of the following:

	Very unlikely	Unlikely	Neutral	Likely	Very likely
Trust strangers	☐	☐	☐	☐	☐
Help those in need	☐	☐	☐	☐	☐
Seek opportunities	☐	☐	☐	☐	☐
Make impulsive decisions	☐	☐	☐	☐	☐
Make intuitive decisions	☐	☐	☐	☐	☐
Wait for something due to me	☐	☐	☐	☐	☐
Deal with adverse circumstances	☐	☐	☐	☐	☐

Question 33. Have you ever been declared bankrupt?

☐ Yes

☐ No

☐ I'd rather not say

Question 34. In the last five years, has a close family member or close friend died?

☐ Yes

☐ No

☐ I'd rather not say

Question 35. In the last five years have you suffered from depression?

☐ Yes

☐ No

☐ I'd rather not say

Question 36. In the last five years have you lost your job?

☐ Yes

☐ No

☐ I'd rather not say

Question 37. In the last five years have you been diagnosed with a serious illness?

☐ Yes

☐ No

☐ I'd rather not say

Question 38. In the last five years have you been a victim of a serious accident?

☐ Yes

☐ No

☐ I'd rather not say

Question 39. In the last five years has your marriage or other close personal relationship broken-up?

☐ Yes

☐ No

☐ I'd rather not say

Question 40. In the last five years have you been a victim of a fraud or scam?

☐ Yes

☐ No

☐ I'd rather not say

Question 41. In the last five years have you been the victim of any other kind of serious crime (such as house breaking, theft, physical assault, or sexual assault?)

☐ Yes

☐ No

☐ I'd rather not say

Thank you for taking the time to complete this survey.

To ensure that your responses are saved, please select 'Finalise' at the bottom of the survey.

If you are worried about anything you mentioned in response to these questions and you want to seek advice or help you can call:

1. Lifeline (131 114)
2. SANE Helpline (1800 187 263)
3. Grief Line (03 9596 7799)

The results of this research will be available from the Australian Institute of Criminology website at www.aic.gov.au

Appendix B: Text of email sent to ACCC survey respondents

Dear Sir/Madam,

According to our records, you have recently lodged a report on the Australian Competition and Consumer Commission's (ACCC) SCAMwatch website.

The ACCC and the SCAMwatch team greatly appreciate your contribution to the collection of scam-related data and thank you for taking the time to lodge your report. The information you provide is used to keep Australians informed about the latest scams in circulation and assists the ACCC in monitoring scam trends and taking action where appropriate.

To further increase our knowledge about consumer fraud and scams, the ACCC has partnered with the Australian Institute of Criminology (AIC) to conduct a research project on consumer fraud victimisation in Australia and the ways in which this type of victimisation might be able to be prevented.

The ACCC and AIC would like to invite you to participate in a survey concerning the details of the report you made to SCAMwatch. The research results will be used to assist with the development of preventive measures and target-oriented awareness programs about consumer fraud. Completing the survey will also help to increase awareness of online scams.

You can complete the survey online by following this link http://www.survey.aic.gov.au/anon/171.aspx. The survey will only take approximately 10 minutes of your time to complete. Participation in this survey is voluntary and anonymous. You can stop participating in the survey at any stage, in which case your responses will not be saved.

The attached page contains information about the survey and also contains contact details for any questions you may have. If you would like to verify the legitimacy of the survey, please contact the ACCC's Infocentre on 1300 302 502, or email the ACCC using the enquiry form on its public webpage www.accc.gov.au.

If you have any questions about the survey content, please contact the Australian Institute of Criminology – by email: scamsurvey@aic.gov.au or phone 02 6260 9202.

I hope that you will be able to take part in the AIC survey.

Yours sincerely,

Delia Rickard
Deputy Chair, ACCC

AIC reports

Research Report

Catherine Emami is a former Research Officer at the Australian Institute of Criminology.

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology and a Professor in the College of Business, Government and Law at Flinders University.

Penny Jorna is a former Research Analyst at the Australian Institute of Criminology.

Australia's national research and knowledge centre on crime and justice

aic.gov.au